MIS Quarterly

RESEARCH ARTICLE

WHAT DO SYSTEMS USERS HAVE TO FEAR? USING FEAR APPEALS TO ENGENDER THREATS AND FEAR THAT MOTIVATE PROTECTIVE SECURITY BEHAVIORS[1]

Scott R. Boss
Department of Accountancy, Bentley University, 175 Forest Street,
Waltham, MA 02452 U.S.A. {sboss@bentley.edu}

Dennis F. Galletta
Katz Graduate School of Business, University of Pittsburgh, 282a Mervis Hall,
Pittsburgh, PA 15260 U.S.A. {galletta@katz.pitt.edu}

Paul Benjamin Lowry
College of Business, City University of Hong Kong, P7718, Academic 1,
Hong Kong, CHINA {Paul.Lowry.PhD@gmail.com}

Gregory D. Moody
University of Nevada, Las Vegas, 329 Frank and Estella Beam Hall, 4515 S. Maryland Parkway, Mail Stop 6034,
Las Vegas, NV 89154 U.S.A. {gregory.moody@unlv.edu}

Peter Polak
Department of Decision Sciences & Information Systems, College of Business, Florida International University,
11200 S.W. 8th St., RB 250, Miami, FL 33199 U.S.A. {ppolak@fiu.edu}

Because violations of information security (ISec) and privacy have become ubiquitous in both personal and work environments, academic attention to ISec and privacy has taken on paramount importance. Consequently, a key focus of ISec research has been discovering ways to motivate individuals to engage in more secure behaviors. Over time, the protection motivation theory (PMT) has become a leading theoretical foundation used in ISec research to help motivate individuals to change their security-related behaviors to protect themselves and their organizations. Our careful review of the foundation for PMT identified four opportunities for improving ISec PMT research. First, extant ISec studies do not use the full nomology of PMT constructs. Second, only one study uses fear-appeal manipulations, even though these are a core element of PMT. Third, virtually no ISec study models or measures fear. Fourth, whereas these studies have made excellent progress in predicting security intentions, none of them have addressed actual security behaviors.

This article describes the theoretical foundation of these four opportunities for improvement. We tested the nomology of PMT, including manipulated fear appeals, in two different ISec contexts that model the modern theoretical treatment of PMT more closely than do extant ISec studies. The first data collection was a longi-

[1]M. Adam Mahmood was the accepting senior editor for this paper. Thomas Ferratt served as the associate editor. Author order is alphabetical and contributions are shared equally.

The appendices for this paper are located in the "Online Supplements" section of the *MIS Quarterly*'s website (http://www.misq.org).

tudinal study in the context of data backups. The second study was a short-term cross-sectional study in the context of anti-malware software. Our new model demonstrated better results and stronger fit than the existing models and confirms the efficacy of the four potential improvements we identified.

Keywords: Information security, protection motivation theory, system backups, model comparison, fear appeals, threat, coping, intentions, behavior

Introduction

A key focus in information security (ISec) research is finding ways to motivate end users, employees, and consumers to improve protection of their individual and organizational information assets. The theoretical approaches recently used to encourage security compliance include general deterrence theory (GDT; e.g., Herath and Rao 2009; Hu et al. 2011), rational choice theory (RCT; e.g., Bulgurcu et al. 2010; Hu et al. 2011), accountability theory (Vance et al. 2013, 2015), reactance and justice theories (Lowry and Moody 2015; Lowry et al. 2015; Posey et al. 2011; Wall et al. 2013), and protection motivation theory (PMT; e.g., Crossler and Bélanger 2014; Herath and Rao 2009; Lee et al. 2008; Lee and Larsen 2009). The bulk of recent ISec literature on compliance resulting from sanctions, threats, or fear represents a shift from earlier GDT-based approaches to a stronger emphasis on PMT (Crossler et al. 2013). A key reason for this shift is that GDT and RCT are based on a foundation of command and control, whereas PMT is based on the idea of using persuasive messages that warn of a personal threat and describe countervailing measures that consist of protective behavior (Floyd et al. 2000). PMT is naturally suited for ISec contexts in which end users, employees, and consumers require additional motivation to protect their information assets. Several ISec studies that use PMT as the primary basis for theory development have been published recently in information systems (IS) journals (Herath and Rao 2009; Jenkins et al. 2013; Johnston and Warkentin 2010a; Lee et al. 2008; Lee and Larsen 2009; Liang and Xue 2010).

These studies have made notable contributions in advancing PMT-based research in the ISec context; however, the literature has not fully leveraged PMT research conducted in fields outside IS to provide a wider range of opportunities for theory and practice. In our review, we found four unleveraged opportunities in extant ISec PMT research. First, although the studies use many of the PMT concepts, none of them use all of its core constructs, and some deviate dramatically from PMT without proper theoretical justification. Second, with few exceptions (e.g., Johnston and Warkentin 2010b; Johnston et al. 2015), none of the studies manipulate an actual fear appeal in the context of the research. Third, although the existing non-ISec PMT research has supported fear as a key partial mediator in PMT (e.g., Floyd et al. 2000; Rogers and Prentice-Dunn 1997), no ISec PMT-related research has measured fear to examine the efficacy of a manipulated fear appeal. Fourth, the majority of ISec studies focus on behavioral intentions and not on actual security behaviors.

The purpose of this paper is to perform an extensive review of PMT and its conventional practice in ISec research to identify opportunities for potential theoretical and methodological improvements on which to build this literature. Notably, we not only identify and explain these opportunities, but also propose theoretically and empirically addressable research questions and provide results based on empirical testing in two different studies, each with a different security context. Study 1 involved a longitudinal study that used the main constructs of PMT, which we term its *core nomology* based on Milne et al. (2002), and added fear appeals and the experience of fear itself in the context of data backups. Study 1 was useful in reintroducing the impact of fear appeals and the fear construct to PMT and assessing actual behavior along with intentions.

Study 2 applied the *full nomology* of PMT (using all potential PMT constructs; that is, all Study 1 constructs as well as maladaptive rewards) to a malware context in a short-term cross-sectional experimental survey. Like Study 1, Study 2 included manipulated fear appeals and the measurement of actual behaviors. However, Study 2 added measurement of maladaptive responses, which we describe later. The results of both studies show improved model-fit statistics when compared to less-complete models or approaches.

This paper begins by examining the theoretical background that serves as the foundation for PMT and reviewing the full nomology and basic causal mechanisms of the theory. On this theoretical basis, we then review ISec PMT studies published in major journals and examine the extent to which the authors have applied PMT's core nomology. Next, we investigate the four research opportunities by examining the results of both studies. The paper then presents the methodology, results, and implications in terms of those research opportunities, and concludes with a discussion of contributions to theory, research, and practice.

Approaches to PMT and Fear-Appeals Research

Several approaches to fear appeals have been taken to persuade people to embrace certain intentions or actions. Simply put, *fear appeals* "are persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends" (Witte 1992, p. 329). For decades, psychologists have studied why people respond or fail to respond to a message contained in a fear appeal compared to individuals who do not receive any specific fear appeal (Witte 1992). Fear-appeals research has frequently focused on PMT. In this section, we briefly explain the theoretical foundation that preceded PMT, which provides insights into the underlying assumptions and boundary conditions of the theory. We then describe PMT models with an emphasis on their most recent implementations.

The fear-as-acquired-drive model (Hovland et al. 1953) was the earliest attempt to address people's motivations for acquiescing to persuasive messages. This theory posits that fear or emotional tension functionally drives individuals toward a desired behavior (de Hoog et al. 2007). The main contribution of this model is its focus on defensive reactions exhibited by individuals after receiving a fear-inducing recommendation (de Hoog et al. 2007). When a message induces fear, an individual may find that adopting the desired behavior will reduce or mitigate that fear. However, if following that path does not provide the desired amelioration, the person may judge the recommendation as ineffective or impossible to execute. In this scenario, the individual will search for alternate solutions to reduce fear (Witte 1992, 1994).

Building on this drive-reduction model, the parallel process model (PPM) (Leventhal 1970) focuses more on the cognitive responses of individuals confronted with a fear-inducing recommendation. Consequently, this model is the most direct predecessor of PMT. PPM posits that threats are cognitively evaluated and result in two parallel processes: fear control and danger control (de Hoog et al. 2007). *Fear control* includes responses such as denial or avoidance that reduce the unpleasant feelings evoked by the message, thus providing little help in dealing with the actual threat. Conversely, *danger control* attempts to cope directly with the danger and lessen its impact (de Hoog et al. 2007; Leventhal 1970). The main contribution of PPM was its enhancement and clarification of the processes mediating fear-arousing communications, which it substituted for a focus on fear itself as the central cause of behaviors. However, the theory does not specify which conditions lead to either fear control or danger control, how the two processes interact, or how individuals alternate between the two processes (de Hoog et al. 2007).

PMT grew out of the foundation of fear-appeals research in PPM. PMT includes the concept in PPM of danger-control response and further explains what can be done to enhance people's ability to cope with danger in a constructive manner. Those *adaptive responses* (Rogers 1975, 1983) are desired behaviors that decrease the targeted threat and are also referred to in the literature as *danger controls* (Rogers 1983). However, the original formulation of PMT essentially omits any consideration of *maladaptive responses*—making it distinct from parallel response models such as PPM. Maladaptive responses are undesired behaviors intended only to decrease fear (for example, by denying or discounting the danger) but not the danger posed by the threat. These responses are also known as *fear control* (Rippetoe and Rogers 1987).

PMT has been enhanced and extended over time in many articles; we used the most recent version, for which the comprehensive meta-analysis by Floyd et al. (2000) found strong support. PMT is of particular interest for our study because it has been adapted several times to the ISec context (e.g., Herath and Rao 2009; Johnston and Warkentin 2010a; Lee et al. 2008; Lee and Larsen 2009; Liang and Xue 2010). Before explaining the research opportunities found in these adaptations, we further describe the assumptions and boundary conditions of PMT.

Central to PMT is an understanding of the concept of *protection motivation*. A leading PMT theoretical review and meta-analysis concluded that "the protection motivation concept involves any threat for which there is an effective recommended response that can be carried out by the individual" (Floyd et al. 2000, p. 409). The main contribution of PMT is its capacity to predict users' intentions to protect themselves *after* receiving fear-arousing recommendations: "The purpose of PMT research is usually to persuade people to follow the communicator's recommendations; so, intentions indicate the effectiveness of the attempted persuasion" (Floyd et al. 2000, p. 411). Figure 1 depicts the cognitively mediating processes of PMT along with its core- and full-construct nomologies.

Threat appraisal and coping appraisal, the two components of PMT shown in Figure 1 that shape protection intentions, form the core assumptions of PMT. The basic idea of PMT is that a fear appeal triggers the threat-appraisal process. Two processes and outcomes must occur for a person to engage in an adaptive response: First, in the threat-appraisal process, the threat and generated fear that inspire protection motivation must be weighted more heavily than maladaptive rewards earned by not engaging in protection motivation. Second, in the coping-appraisal process, a person's response efficacy and self-efficacy must outweigh the response costs for engaging in the protection motivation. In terms of threat appraisal, it is

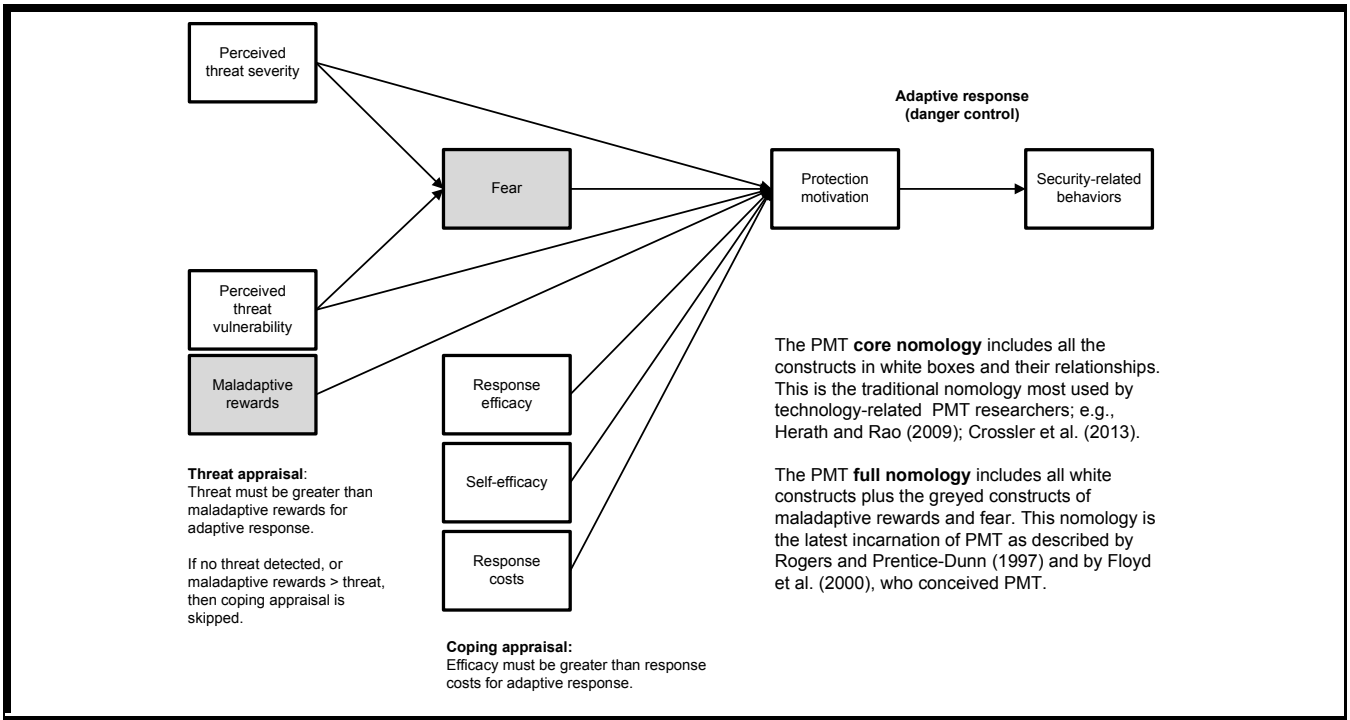

Figure 1. Overview of the Core and Full Nomologies of PMT

important to emphasize that the feeling of fear is conceptually distinct from the fear appeal or fear-appeal message. In a PMT context, *fear* is defined as a "relational construct, aroused in response to a situation that is judged as dangerous and toward which protective action is taken" (Rogers 1975, p. 96). Separately, a *fear appeal* is the stimulus designed to trigger both fear and the threat-appraisal and coping-appraisal processes (Floyd et al. 2000; Fry and Prentice-Dunn 2005, 2006; Milne et al. 2000; Rogers 1983). Ideally a fear appeal does not just increase threat but would also increase efficacy by giving a respondent a path to address the threat. Importantly, the best fear appeals create both high threat and high efficacy because they address both the threat and the individual's ability to deal with it (Milne et al. 2000; Witte and Allen 2000). The fear-appeals literature uses the message (fear appeal) as a manipulation. We further discuss these components and the associated construct definitions in the theory section.

The assumptions and foundations of PMT are highly relevant to behavioral ISec research and practice. Accordingly, several noteworthy studies have embraced derivations of PMT for this context. Table A1 in Appendix A summarizes our review of ISec research that uses derivations of PMT. For each study, this table indicates key PMT constructs that are not used, non-PMT constructs that are added, and other decisions that conflict with PMT. Although these studies make useful contributions to the literature, we find that no published ISec PMT article can be classified as adhering fully to PMT. Our review points to four research opportunities: (1) using the PMT nomology, (2) using fear appeals, (3) measuring fear, and (4) measuring actual behavioral changes, not just intentions. The promise of the last opportunity is self-evident, so we develop it further in the hypothesis section. However, the first three opportunities require further explanation prior to hypothesis development.

Opportunity 1: ISec Research Can Be Improved by Using the Core Nomology of PMT

A key issue is that virtually every ISec study made major, unsupported adaptations to PMT without (1) testing the core PMT nomology or (2) demonstrating that its changes actually improve the explanatory power of PMT or that the alternative model it developed enjoys better model fit than PMT. Typically, ISec studies omit core PMT concepts or fear-appeal manipulations without explanation. Some constructs such as response costs and response efficacy are commonly dropped, and researchers do not provide adequate justification for such exclusions. Constructs are also renamed, defined, and measured in nonstandard and perhaps incorrect ways that receive little or no testing. To serve as a useful guide in our

review, Appendix C defines all of the key constructs in this literature that we apply in our model.

Additionally, many of the studies add new constructs that are external to the PMT nomology. Moreover, these studies often incorrectly cite as PMT theories several models that actually depart so greatly from PMT that they are more aptly labeled PMT spinoffs. Four categories of PMT spinoffs emerged in our review, and we explain them in detail at the end of Appendix A: (1) the technology threat avoidance theory (TTAT) model, as proposed by Liang and Xue (2010); (2) the fear-appeals model (FAM), proposed by Johnston and Warkentin (2010a); (3) extensions to the health belief model (HBM) developed by Ng et al. (2009) and Claar and Johnson (2012); and (4) various efforts to create unified models that merge parts of PMT with other theories, such as those proposed by Herath et al. (2012) and Herath and Rao (2009).

Although adding non-PMT constructs to PMT models or creating PMT spinoff models can provide valuable explanatory power, it can also distance the resulting model from PMT in ways that are not theoretically justified. Consequently, although these additions are promising, it is impossible to know whether the proposed models offer a better theoretical and empirical fit than a nomology truer to PMT. These researchers cannot clearly demonstrate whether the described models actually improve or expand upon PMT or simply switch out proven constructs for new ones. This limitation occurs because the studies do not provide the model-fit statistics required to demonstrate that an extended model improves on a baseline model. By using at least the core, established PMT nomology fully, ISec researchers may be able to increase the explanatory power of their models and may find that non-PMT additions are neither helpful nor necessary.

Opportunity 2: ISec Research Can Be Improved by Including Fear-Appeal Manipulations

Although the link between threat and fear seems straightforward, ISec PMT-related research generally has ignored fear appeals and has not measured fear to examine the efficacy of threats. Only two related studies actually incorporated fear appeals (Johnston and Warkentin 2010a; Johnston et al. 2015), even though the use of fear appeals is a fundamental assumption of PMT research (Floyd et al. 2000; Rogers 1983; Rogers and Prentice-Dunn 1997).

This gap creates an inherent conflict with the contextual assumptions of PMT, in which threats and fear generated by a fear-appeal message are intended to persuade a person to perform a protective behavior. Recently, in a treatise on security research opportunities, Crossler et al. (2013) emphasized that fear must be delivered through a manipulation (at minimum) of the threat's severity and vulnerability. Without introducing any elements of fear, a study cannot easily determine whether fear and fear appeals are appropriate for a given ISec context (Crossler et al. 2013).

Opportunity 3. ISec Research Can Be Improved by Measuring Fear

No ISec study has measured actual fear, as currently modeled by PMT. Measuring fear helps researchers know whether the threat severity and vulnerability generate an appropriate level of fear. That is, without measuring fear, the effectiveness of an appeal cannot be assessed directly, only indirectly (LaTour and Rotfeld 1997; Witte 1992, 1994; Witte and Allen 2000). This point is important, because what is perceived as threatening obviously varies greatly from person to person, and individuals must perceive a salient threat stimulus to experience a level of fear (LaTour and Rotfeld 1997; Witte and Allen 2000).

Notwithstanding assumptions to the contrary, fear can indeed be measured in behavioral research. A substantial body of PMT, psychology, and social psychology research has shown that fear is an emotion with strong cognitive, affective, and physical manifestations and that it is readily measurable by self-report (Leventhal 1970; McIntosh et al. 1997; Osman et al. 1994; Rogers 1975; Witte 1992, 1998; Witte et al. 1996). Hence, omitting fear from the full PMT nomology is unnecessary and could undermine ISec research.

Explication of PMT Hypotheses in the Security Context

Overview of the Research Model

To respond to the issues and opportunities identified in the previous section, we propose that for ISec contexts, a PMT model must be characterized by the following properties and assumptions: (1) at minimum, it uses the core nomology of PMT; (2) it is designed and tested through a manipulated fear appeal; (3) it models fear as a partial mediator and actually measures that fear through a self-report to observe whether it is salient in the context of the model; and (4) in addition to intentions, it measures actual protective behaviors as a more complete test of the efficacy of PMT.

Two other important choices in our model need to be emphasized. First, PMT has evolved over time. Although the original version (Rogers 1975) was abandoned long ago, it is often incorrectly cited and used in ISec literature. A second version is closer to the current one, but omits some key changes related to fear, and thus is also often incorrectly used (Maddux and Rogers 1983; Rogers 1983). In this version, self-efficacy (from social cognitive theory) was brought in, as well as the idea of maladaptive rewards. The idea of fear was recognized but downplayed. This second version is what we refer to as the *core* PMT model.

The third and latest version extended PMT to more strongly emphasize maladaptive rewards and reinstated fear as an important partial mediator (Floyd et al. 2000; Rogers and Prentice-Dunn 1997). Although these changes do not alter the structure of the core constructs of PMT, we refer to this approach as the *full* PMT model, depicted in Figure 1. We differentiate PMT this way in particular because most IS research only considers the core PMT and ignores the additional elements of the full PMT model.

Following leading modeling literature on combined process-variance models (Burton-Jones et al. 2015; Markus and Robey 1988; Tsohou et al. 2008), another important pragmatic decision on our part is to describe PMT as a variance model with a process model component in which the threat-appraisal process must occur and be considered first, followed by a consideration of the coping-appraisal process (Floyd et al. 2000; Rogers and Prentice-Dunn 1997). None of the extant ISec literature has created a PMT model that can be tested as a variance model with a process model component, but has instead relied on simplified variance versions of PMT. We are able to tease out the process component by leveraging subgroup analysis with structural equation modeling (SEM) to account for those who do not receive the same level of threat appraisal and fear appeal. We further explain and propose our full PMT model in this section.

The PMT model for hypothesis testing, presented in Figure 2, includes all relationships from both the core and full PMT models described earlier. Most of the hypotheses posited below apply to both models, but some apply only to the full model, as clearly distinguished in the figure. Namely, the full model adds the consideration of both fear and of maladaptive rewards. These two items could assist in explaining more of the variance in intentions, but we acknowledge the possible risk involved in their measurement. Measuring the items might (1) sensitize study participants to a risk and (2) alter their reactions in a manner that would not exist outside of a study. For instance, asking a person if he or she is afraid might actually invoke more fear outside the context of the study; conversely, it might present a challenge to minimize or set aside the fear. It can therefore be argued that the core model might provide a safer, more realistic setting for a study in the IS field, so both versions might need to be tested. In our studies, fear was not considered to pose a measurement problem and was expected to be rather stable after the fear appeals were provided, but maladaptive rewards were not assessed in Study 1, which focused on backups. Given that Study 1 was a longitudinal study and provided dozens of opportunities to make backups, maladaptive reasons for failing to make backups were likely to change several times during the data-collection period. Therefore, our two studies differ with respect to the inclusion/exclusion of maladaptive reward measurements.

Theoretical Support and Hypothesis Development for the Research Model

We begin by further explaining the two appraisal processes that form the foundation of PMT: threat appraisal and coping appraisal. A threat appraisal consists of both vulnerability, the degree to which an individual believes the threat applies to his or her specific circumstances or the probability that the described threat will occur (Rogers 1983), and severity, the degree to which an individual believes the threat will cause consequential harm (Rogers 1983).

H1a. *An increase in perceived severity of threat increases protection motivation.*

H1b. *An increase in perceived vulnerability to threat increases protection motivation.*

If one perceives a relevant and severe threat, then *fear*, a negative emotional response, is generated as an outcome. Therefore, threat severity and threat vulnerability predict fear (Floyd et al. 2000; Rogers and Prentice-Dunn 1997), which acts as a partial mediator in the full model shown in Figure 2. Therefore, we posit that:

H2a. *An increase in perceived severity of threat increases perceived fear.*

H2b. *An increase in perceived vulnerability to threat increases perceived fear.*

Combined with threat, fear plays a further, special role in PMT, as shown in Figure 2. A PMT study should thus ideally introduce a strong fear appeal. If fear can be realistically measured, its role in mediating the relationship between threat and protection motivation can be explored.

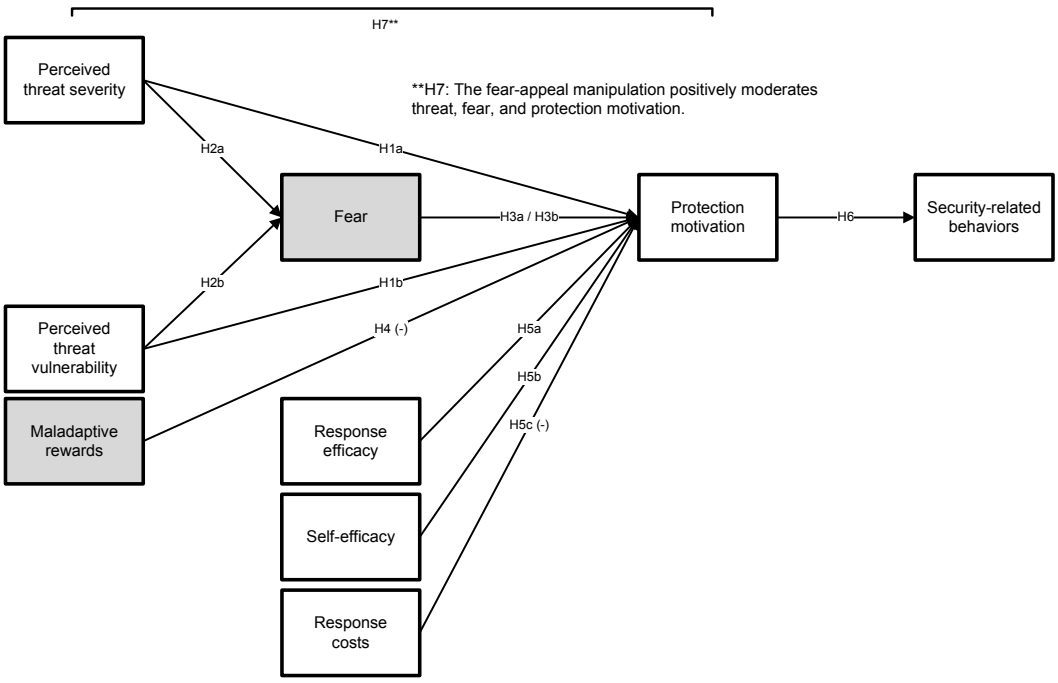

Figure 2. PMT Model for Hypothesis Testing, Including Core and Full PMT Nomologies

Invoking fear can lead a person to take protective instructions more seriously (Leventhal 1970; McIntosh et al. 1997; Osman et al. 1994; Rogers 1975; Witte 1992, 1998; Witte et al. 1996). If the message is not even seen, however, then the person's behavior might be based on incomplete or incorrect information. Because the message could be ignored, the measurement of fear will be useful to researchers as long as it does not sensitize participants to the means and goals of the study. Therefore,

H3a. An increase in fear increases protection motivation.

H3b. Fear should act as a partial mediator between threat and protection motivation.

A potentially important part of the threat-appraisal process is that the evaluation of maladaptive rewards can have an impact on the threat-appraisal process (Floyd et al. 2000; Rogers 1983; Rogers and Prentice-Dunn 1997). A *maladaptive reward* is any kind of reward for the response of not protecting oneself, such as a perhaps mistakenly perceived time or cost savings, as well as pleasure or even sabotage (Floyd et al. 2000; Rogers and Prentice-Dunn 1997). If the rewards outweigh the perceived threat, a person may choose the maladaptive route of not following the desirable protective behavior

H4. An increase in maladaptive rewards decreases protection motivation.

Threat and the associated fear can motivate adaptive behavior if a person feels capable of coping with the threat to "avert the threatened danger," and they are not considered if the threat-appraisal process fails to be triggered because of an unnoticed or unimportant threat (Floyd et al. 2000, p. 410). This *coping-appraisal* process considers three variables: self-efficacy, response efficacy, and the costs of performing the adaptive behavior (the response recommended in the fear appeal) (Floyd et al. 2000; Rogers 1983). *Response efficacy* is the degree to which a person believes that the recommended response will be effective (Maddux and Rogers 1983). *Self-efficacy* is the degree to which an individual believes that he or she has the capability to perform what is required to avert the threat (Maddux and Rogers 1983). Finally, *response costs* are any perceived direct personal costs (e.g., effort, time, money, or trouble) incurred by the individual by taking protective steps (Floyd et al. 2000). For a positive coping-appraisal response, it is necessary for people to believe that (1) the desired response will be effective (i.e., response effi-

cacy), (2) he or she will be able to perform the action (i.e., self-efficacy), and (3) the costs of performing the action will not exceed the perceived benefits (i.e., response costs).

H5a. An increase in response efficacy increases protection motivation.

H5b. An increase in self-efficacy increases protection motivation.

H5c. An increase in response costs decreases protection motivation.

In PMT research, the primary theoretical focus has been predicting intentions toward protection motivation (Floyd et al. 2000; Rogers 1983; Rogers and Prentice-Dunn 1997). However, outside of ISec research, PMT has been efficaciously extended to predict behaviors (Floyd et al. 2000). Hence, leading PMT-based health research examines actual behavioral change, not just intentions (e.g., Fry and Prentice-Dunn 2006; Milne et al. 2000). We argue that actual behaviors are useful for ISec research because the goal is to change security behaviors, not just to increase protection motivation (Crossler et al. 2013). We thus assert that to increase application to practice, an efficacious test of the full nomology of PMT should also include a test of actual behaviors. That being said, PMT meta-analysis indicates that protection motivation should be the strongest predictor of behavioral change (Milne et al. 2000). Thus,

H6. An increase in protection motivation increases security-related behaviors.

Outside of IS, it is a recognized practice in PMT research to provide experimental manipulations of both high and low fear appeals. Milne et al. (2000) reported that most studies include a weak versus strong fear appeal manipulation, as opposed to one that is absent versus present. This approach provides at least a base-level awareness of a threat, and provides a fair comparison between the two groups. Participants who are completely unaware of a threat cannot be expected to experience constructs such as fear, maladaptive rewards, or response efficacy when the participant has no basis upon which to respond. Importantly, such a case violates a key assumption of PMT that a person be aware of a threat and that it be relevant; otherwise, the coping appraisal process does not occur and PMT does not apply (Rogers 1983; Rogers and Prentice-Dunn 1997).

Consequently, it is important to treat stronger and weaker fear appeals properly in a theoretical model. Alternatives are to provide the fear appeal as antecedent to fear in the model, to depict the fear appeal as a moderator of many or most relationships in the model, or to treat the fear appeal as the central moderator of an entire model by splitting the model into subgroups. The fear appeals literature itself discounts the first approach in that the fear appeal affects constructs throughout the entire model and not just the initial set of constructs that make up threat appraisal (Rogers 1983; Rogers and Prentice-Dunn 1997). The second approach becomes infeasible given the number of relationships in SB-SEM, which sharply reduces degrees of freedom and dramatically increases covariance from the collinearity of interactions terms, as commonly assessed by the variance inflation factor. Regardless, model fit statistics will be entirely unsupportive of such a model due to the increase in χ^2 variance that is not equally predicted by the changes in the model.

Leadership with this issue is found in a paper by McClendon and Prentice-Dunn (2001) that conducted a follow-up study looking back on pretest and posttest subgroups. The authors did not use SEM, but presented levels of variables separately. It was striking that the levels of *all* variables in the PMT model changed significantly in predicted directions from pretest to post-test; and, after a one-month follow-up, vulnerability, perceived severity, response efficacy, self-efficacy, and two different intentions scores all increased, and with the exception of self-efficacy, *remained* at their high post-test levels. Likewise, rewards and response costs decreased and also remained at their lower levels at the follow-up date. Because many of these variables are depicted at several stages in the PMT model, their analysis suggests a whole model impact of a fear appeal. Although relationships were not tested, the impact of fear appeal on all variables suggests that the impact of a fear appeal does go beyond a fear construct alone.

Aside from their work, there is a fundamental theoretical justification for a fear appeal influencing the entire PMT model. Recall that an effective fear appeal will provide messages that will not only describe the problem (increasing threat and subsequent fear) but also a solution (increasing efficacy and driving an adaptive-coping response) to address the individual's ability to deal with it (Milne et al. 2000; Witte and Allen 2000). Thus, both threat and efficacy are core to the threat- and coping-appraisal processes that drive PMT. Because PMT is partly a process model and partly a variance model, an effective fear appeal drives the entire adaptive coping response, which is key to PMT. Nonadaptive responses are fundamentally outside the scope of the model (Rogers 1983; Rogers and Prentice-Dunn 1997; Witte 1994). In the case of McClendon and Prentice-Dunn (2001), they further demonstrate that repeating the fear-appeal message makes it even more effective.

Given that there are nine relationships in the model, three representative examples can be useful to illustrate this whole

model moderation approach. They are representative because they provide all possible combinations of activation of threat severity and response efficacy. We theorize that the other relationships will behave similarly. In H1(a), the fear appeal moderates the relationship between severity and intention because the impact of severity can be magnified if a user has been exposed to one or more messages that include recommendations for action. In H5a, response efficacy will more strongly influence protection motivation for those who have been exposed to the fear appeal because, while they might understand their ability to respond, they need to fully recognize the threat provided in the fear appeal. Finally, in H6, while intentions are usually considered to lead to behavior, those with a strong fear appeal will be more likely to act on their intentions because they have full understanding of both the threat and an efficacious response to the threat. Therefore, stated in broad terms,

H7. The greater the strength of a fear-appeal manipulation, the stronger the relationships in the model in predictions of fear, intention, and behavior.

This approach, closely tied to the basics of PMT, points to a key opportunity in ISec research, because only one set of authors to date have used fear appeals (Johnston and Warkentin 2010a; Johnston et al. 2015). Notably, the results of these external manipulations might not be discernible when data from both strong and weak fear-appeal treatments are combined into a single path model. We thus add an additional test by creating and comparing subsamples based on the high fear-appeal manipulation and the low fear-appeal manipulation. Namely, if PMT holds well in an ISec context, the high fear-appeal manipulation should result in higher threat, fear, and protection motivation, and in stronger relationships throughout the model, than would a low fear-appeal manipulation.

Methodologies

To achieve the increased generalizability necessary for an improved PMT model that addresses the identified research gaps, we conducted empirical studies in two different ISec-specific contexts. The first used fear appeals in a longitudinal design in an attempt to motivate participants to make backups to protect their computing resources. Because of the longitudinal nature of the study and the difficulty of measuring maladaptive rewards in literally hundreds of different settings, the core nomology of PMT was adopted, and, in addition, fear was measured following a comfortable interval after the last fear appeal was provided. The second study was a cross-sectional field experiment that used deception in an attempt to increase participants' use of anti-malware software. Both studies included fear appeals, fear, and actual behavior; the second study also measured maladaptive rewards to achieve the full PMT nomology.

Methodology for Study 1: Backups

Study 1 Participants

MBA students, collectively enrolled in four sections of a required introductory IS course, were invited to participate for extra credit. Of the 195 students in those sections, 125 (64%) volunteered to participate, and 104 participated fully. Respondents ranged in age from 21 to 44 years, and all had at least a bachelor's degree. The sample consisted of 38 women (37%) and 66 men (63%). Additionally, of the people who chose to participate, only 21% did not perform any backups during the data collection period, whereas 79% performed at least one backup. These proportions did not vary, irrespective of whether the participants received software from the researchers to perform backups to a remote server or were expected to use their own software. Other descriptive statistics for the sample are shown in Table 1. The study received institutional review board approval, and participants in the study provided informed consent.

Study 1 Design

Participants were segmented by study-group blocks to reduce potential contamination of the treatment via communication about the fear appeals. Each block was assigned randomly to two cells: high (strong) fear appeal or low (weak) fear appeal. All were asked to keep manual logs recording their backups and the dates of those backups in a spreadsheet provided by the researchers. In addition, half of the participants received software to automate the backup process, making it possible to compare the logs against the self-reports to assess accuracy. The introductory discussion of backups and the distribution of backup software took place at the beginning of the course.

Study 1 Fear-Appeal Manipulations

The study manipulated the presence of fear appeals with two treatment conditions: high and low fear appeal. Participants in the low fear-appeal condition received only minimal messages regarding the importance of backups. Early in the semester, all participants saw a humorous, low-key commercial that stated that it was important to back up data. Partici-

Table 1. Respondents' Demographic Characteristics

Characteristic (Years)	Mean	SD	Min	Max
Computer use	13.50	4.94	5	25
Age	26.78	4.72	21	44

Table 2. Effectiveness of Fear Appeals: Study 1

Condition	n	Severity	Vulnerability	Fear	Intention	Backups
Full sample	104	5.42 (1.48)	4.08 (1.34)	3.64 (1.98)	4.33 (1.85)	5.42 (8.54)
High fear-appeal subsample	56	5.57 (1.29)	4.11 (1.37)	4.13 (1.52)	4.71 (1.91)	7.66 (10.94)
Low fear-appeal subsample	48	5.305 (1.63)	4.04 (1.31)	3.37 (2.27)	4.01 (1.76)	3.52 (5.12)
Z statistic (test of significance between high and low fear appeals)		0.96 (ns)	0.25 (ns)	2.01*	1.99*	2.67**

*p < .05, **p < .01, ns = nonsignificant; first numbers in cells are means; numbers in parentheses are SDs

pants in the high fear-appeal condition, however, received more explicit and more numerous messages during the semester regarding actual statistics about the frequency of data loss and the potential expense and harm that such data losses could cause in their personal lives. Participants received these fear appeals three times, or roughly once per month. (See Table 2.)

It is crucial to note that the low fear-appeal condition should not be considered a "no fear-appeal" condition. There is widespread general knowledge that data can be lost due to theft, damage, or equipment failure. However, such an event is rare and does not usually occur immediately after data backup or the failure to do so. Without a potential for data loss, PMT would be irrelevant; for motivation about protection, one needs to be aware of the need for that protection.

The fear appeals appear to have had a significant influence on perceived fear, intentions to back up data, and actual data backups performed. Although the participants in the two subsamples did not perceive any noticeable difference in the severity of the perceived threat, we believe that the manipulation was successful because it altered the expected outcomes between the groups, as evidenced by the fact that the high-fear-appeal subsample consistently exhibited higher scores for each construct than the low fear-appeal subsample. Table 2 further illustrates that the combination of the two subsamples might have increased the unexplained variance within the model and thus obscured these key differences. These outcomes further demonstrate the importance of measuring the fear resulting from the fear appeal.

Study 1 Procedures

Respondents were briefed that they would be required to fill out questionnaires and keep a diary of when they made backups of their data over an eight-week period. In addition to the humorous video about the importance of data backup, the participants were told briefly that all hard drives fail eventually and that theft was a common issue with laptops. This low fear-appeal message was intended to give respondents a basic reason to keep their important data backed up, not to raise their fear to a high level.

Respondents recorded their actual file-backup activity on the provided spreadsheet over an eight-week period, which was to be submitted to the researchers as a proof of participation and as the final step necessary to receive extra credit in the course (2% of the grade). The backup software distributed to some users also kept automatic logs whenever it was used to back up a password-protected, encrypted, and compressed version of their data to a remote server. The analysis revealed that the manual logs closely matched the automated logs, with only a few minor differences in dates and times reported. The logs also showed continued use by the same set of participants, which demonstrated persistent behavior and supported a causal link between behavioral intentions measured at the survey date and the actual behavior that followed.

Of the 125 participants who volunteered for the study, 107 completed all of the surveys and logs. Early in the next semester, all participants were debriefed by e-mail about the study. As part of the debriefing, they were asked if there were

any reason why the information they provided should be disqualified. Three participants reported that they were not permitted by their employers to install the software on their laptops, so they were removed from the study. In total, 104 respondents provided usable data for the analysis.

Study 1 Measures

To test the hypothesized relationships, measures were adopted from the literature and modified to assess the constructs described in the research model (Milne et al. 2002). The measures used in this study are summarized in Appendix B. After the final model runs, we applied a few control variables *ex post facto* to check the completeness of our model for model fit. These essentially added no value in terms of improving model fit. They are explained further in Appendix B and the results section.

Study 1 Epilogue

As noted, one of our main criticisms of the ISec PMT literature is its failure to use the core PMT nomology. Although the first study included longitudinal data drawn from a natural situation of computer usage, it did so by assessing only a general feeling of fear rather than a focused wave of fear and maladaptive rewards at a single decision point. It was thus useful to conduct Study 2, which provided the full nomology in a context that required a single response to a prompt—enabling us to inform theory further by focusing on fear and maladaptive rewards at a particular moment we could control tightly.

Methodology for Study 2: Anti-Malware Software Use

Study 2 Participants

Our volunteer participants were recruited from an undergraduate pool of psychology students at a large university in the United States who were required to complete a certain number of experimental hours as part of their coursework. A total of 327 students participated. Of these, 173 (52.9%) were men and 154 (47.1%) were women. The average age was 20.13 years (SD = 1.99 years), and the average work experience was 0.54 full-time years (SD = 1.46 years). This study was approved by the university's institutional review board.

Study 2 Design

Our second study was designed as a field experiment in which threat severity was manipulated by means of displaying an unexpected virus-warning message while participants browsed a website. Two levels of threat severity (high and low) were used; a control group received no manipulation.

Study 2 Fear-Appeal Manipulations

To manipulate threat severity, the website for the experiment showed an overlay pop-up window with a virus-warning message two minutes after the beginning of the experiment. The user was given details about the severity of the threat and the likelihood of being able to resolve the threat, and was asked to remove the malware by pressing the "OK" button, which would indicate acceptance of the message. The pop-up window was implemented as an in-page overlay element to circumvent pop-up blocking software on the participants' devices, and it was designed to match closely the window style of the participants' operating system environments. For example, the pop-up window had a standard closing button in the top border (an "X" in the upper-right corner for Windows machines and a red dot in the upper-left corner for Macs), in addition to the conventional "OK" button at the bottom of the warning message. The pop-up window was centered on the screen and contained textual and graphical elements that indicated the particular treatment condition. Figure 3 shows an example of the screen-shot manipulations.

Threat severity (high/low) was operationalized with headings indicating a high-risk or a low-risk threat level (catastrophic or harmless) along with a description of the expected consequences of the respective virus. The high-threat "Exterminator" would wipe out the hard drive, resulting in data loss, whereas the low-threat "DumbUser" would make a benign change in the computer's username after a month. The graphical element that manipulated the threat level was a threat meter with an "Extremely Harmful" indication for a high-level threat and a "Harmless" indication for a low-level threat.

To test our fear-appeal manipulation on the participants, we compared the effects produced by the fear appeal, as previously described in Study 1. Table 3 summarizes this manipulation check. Our manipulations were statistically significant and in the right direction. Thus, the manipulation of the fear appeals successfully affected the elements of the threat appraisal and fear, and the actual acceptance of the message was executed by clicking the "OK" button to remove the virus, as suggested by the fear-appeal message.

Study 2 Procedures

The participants were informed that the experiment's goal was to study website usability and design; thus, deception was

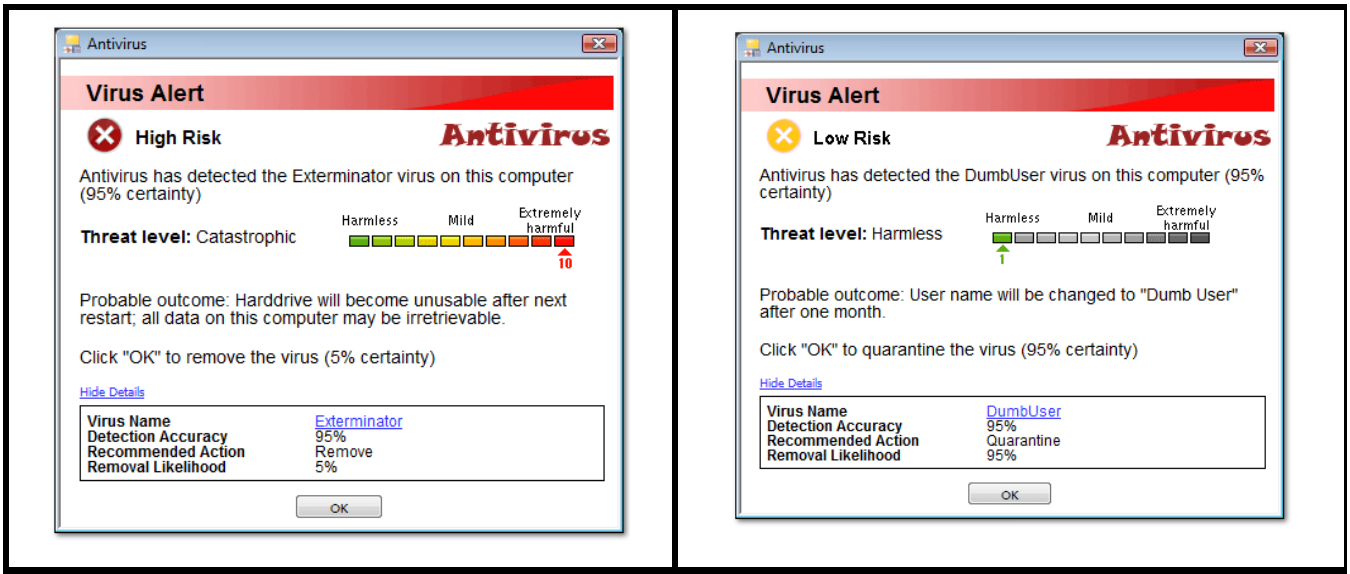

Figure 3. Two Examples of Manipulation

Table 3. Effectiveness of Fear-Appeal Manipulations: Study 2

Condition	n	Severity	Vulnerability	Fear	Intention	Message Accept
Full sample	327	4.16 (1.22)	3.99 (1.18)	2.88 (1.10)	5.28 (1.73)	0.39 (0.47)
High fear-appeal subsample	130	4.27 (1.13)	4.05 (1.16)	3.01 (1.18)	5.32 (1.62)	0.40 (0.49)
Low fear-appeal subsample	142	4.08 (1.29)	3.93 (1.22)	2.80 (1.03)	5.21 (1.79)	0.38 (0.49)
No fear-appeal subsample	55	4.18 (1.34)	3.97 (1.20)	2.77 (1.10)	5.37 (1.95)	n/a
Z statistic (high vs. low)		16.34***	9.56***	18.68***	6.46***	3.97***

***$p < .001$; first numbers in cells are means; numbers in parentheses are SDs

used to increase the realism of the results. Participants were given 10 tasks to complete, all of which were information-search tasks that required them to browse a website for the answers. After completing the tasks, the participants were invited to conclude the experiment by filling out an online questionnaire. A partial copy of a large commercial website that provides articles and reviews about digital photography was created for the experiment. To eliminate the need to place the questions in a separate window, the website layout was modified slightly to accommodate the presentation of the experiment's questions at the top of each webpage. Integrating the questions into the website in this way made the browsing experience more fluid and natural.

After agreeing to join the study, each participant received an e-mail with the web address of the experiment. The experiment could be completed at any time before the deadline, and from any location, using the participant's own computer. To increase external validity, we opted for a field setting instead of a laboratory setting, which allowed participants to use their own devices and therefore increased the perceived impact of the presented threat. This was particularly important, because we wanted to increase the likelihood that the unexpected virus message would be perceived as a legitimate and personal threat. A controlled laboratory setting would have been much more likely to raise participants' suspicions that the message was part of the experiment and would have decreased the malware message's perceived threat, because the threat would have been directed at the university's equipment, not at the participant's personal property (i.e., the hardware, software, and data on the participant's device). Personal relevance of a fear appeal is crucial, as Johnston et al. (2015) recently demonstrated.

Study 2 Measures

As in Study 1, the measures were adopted from the literature and modified to assess the constructs described in the research model. The measures used in this study are summarized in Appendix B. Additionally, we created measures to reflect the actual use and nonuse of the anti-malware software. To do this, we tracked the users' responses to the malware-warning pop-up message that specifically asked for the user's permission to proceed with the malware removal process by requiring them to press "OK." If they pressed "OK," this signaled the intentional use of the anti-malware software. If they closed the browser or pressed "X" to close the pop-up screen, this signaled the intentional nonuse of the anti-malware software. Finally, after the final model runs, we applied a few control variables *ex post facto* to check the completeness of our model for model fit. These variables essentially added no value in terms of improving model fit (see Appendix B).

Analysis and Results

Study 1 Analysis and Results

Convergent and discriminant validities were assessed with confirmatory factor analysis using STATA/SE version 13.1, which was also used for all other tests unless otherwise noted. Model fit was good ($\chi^2_{444} = 923.39$; CFI = 0.974; TLI = 0.964; RMSEA = 0.052; CD = 1.000). Convergent validity was supported by large and standardized loadings for all constructs ($p < .001$) and t-values that exceeded statistical significance. Convergent validity was also supported by calculating the ratio of factor loadings to their respective standard errors, which exceeded |10.0| ($p < .001$).

Discriminant validity was tested by showing that the measurement model had better fit than a competing model with a single latent construct and all other competing models in which pairs of latent constructs were joined. The χ^2 differences between the competing models (omitted for brevity) were significantly larger than that of the measurement model, which was also suggested by the factor loadings, modification indices, and residuals (Marsh and Hocevar 1985). In sum, these tests confirmed that our data had appropriate convergent and discriminant validity.

All composite factor reliability scores exceeded 0.70, suggesting adequate reliability for all constructs. Reliability was also supported in that the average variance extracted (Hair et al. 2006) exceeded 0.70 for all factors. Table 4 summarizes the reliabilities, means, standard deviations, and correlations of Study 1.

Study 1 Model Results

Our STATA model provided common fit indices, which showed that model fit was acceptable for both Study 1 ($\chi^2_{444} = 923.39$; $\chi^2/df = 2.08$; CFI = 0.974; TLI = 0.964; RMSEA = 0.052; CD = 1.000) and Study 2 ($\chi^2_{2107} = 6067.02$; $\chi^2/df = 2.88$; CFI = 0.948; TLI = 0.935; RMSEA = 0.045; CD = 1.000). The results of the model analysis for the full models for Studies 1 and 2 are shown in Figures 4 and 5, respectively (i.e., all manipulations combined into one model).

As shown in Figures 4 and 5, when all the manipulations were combined into an overall model, few of the relationships were significant. Perceived severity and perceived vulnerability were found to significantly influence fear. Response cost and perceived severity were the only consistent predictors of intentions, and intentions predicted behaviors. These results point to the importance of considering the subsamples and the moderation effect of fear (i.e., H7).

In addressing H7, we note that individuals who did not receive the high level of the fear appeal introduced a large degree of unexplained variance in backup intention and subsequent backup behavior in the overall model. This is expected, because many of these participants did not start with a strong perception of threat and were thus not expected to engage in strong and urgent protection motivation behaviors. Importantly, this is the process component of our model, in that high threat must be generated by a fear appeal before a proper coping response can be given. Also, a strong fear appeal will be more effective than a weaker one. Hence, the fear appeal can be seen as a conceptual moderator.

Consequently, the fear appeal gives salience to the fear, threat, and protection motivation constructs in the PMT model. A strong fear appeal provides high salience and a weaker one provides low salience throughout the model (H7). As described earlier, a strong fear appeal is required for perceiving both a need for action, steps for action, and personal efficacy in taking the action. Without accounting for fear appeal strength, unexplained variance could increase, potentially undermining PMT predictions. Thus, we examined the structural models for the high fear-appeal participants and compared them to the results of structural models for the low-fear-appeal participants. We therefore also provide the models in Figures 6 and 7 for high- and low fear-appeal manipulations, respectively.

Importantly, the high fear-appeal manipulation would represent the way fear appeals should ideally be used to increase intention; it is not surprising that the manipulation properly

Table 4. Study 1 Overall Reliabilities, Means, Standard Deviations, and Correlations

Construct	Rel.	Mean	SD	1	2	3	4	5	6
1. Computer self-efficacy	.969	5.30	1.65						
2. Response efficacy	.794	6.31	0.79	.061					
3. Response cost	.769	3.11	1.34	-.112	-.217				
4. Vulnerability	.830	4.08	1.34	-.021	-.002	-.046			
5. Severity	.774	5.42	1.48	-.056	.068	-.169	.008		
6. Fear	.908	3.64	1.98	-.002	.129	-.370	.282	.216	
7. Intent	.832	4.33	1.85	.052	.225	-.575	-.019	.171	.243

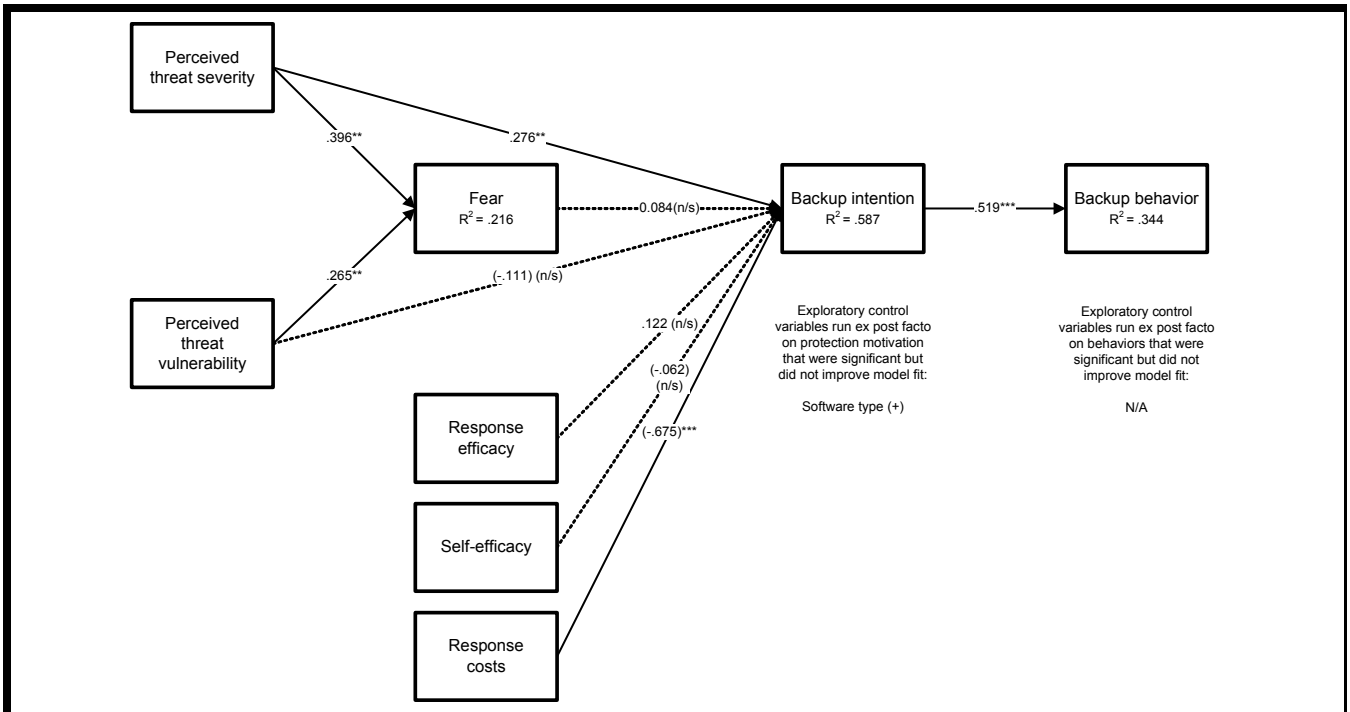

Figure 4. Overall Model Results for Study 1 (All Manipulations Combined): Data Backups

follows the core PMT model with the addition of fear measurement. The high model had an R^2 of .881 for intentions, whereas the low model had an R^2 of .419—meaning that the strong fear appeal doubled its influence on intentions. Moreover, fear played an important role in the high model and no role in the low model. In fact, several PMT relationships are insignificant or are in the wrong direction in the low model and predict a third of the actual behavior of the high model. These results demonstrate the need for a proper fear-appeal manipulation with PMT. Model-fit indices were as follows: high fear-appeal subsample model: $\chi^2_{444} = 898.45$; CFI = 0.941; TLI = 0.943; RMSEA = 0.046; CD =1.000; low fear-appeal subsample model: $\chi^2_{443} = 893.32$; CFI = 0.954; TLI = 0.943; RMSEA = 0.035; CD = 1.000.

Finally, we used ANOVA and MANOVA to investigate whether the two subsamples (high and low fear appeals) did in fact have a systematic effect on the results, and we found that the fear-appeal indicator distinctly predicted intentions for both studies, even when entering all other constructs into the models first. Further, we extracted the correlation matrices for each subsample and found systematic differences between the subsamples. This finding was supported by canonical correlation, which indicated that a majority of the variance between the subsamples was distinct from each other. Having found that the samples exposed to the different treatments are in fact systematically distinct provided further support for analyzing them separately.

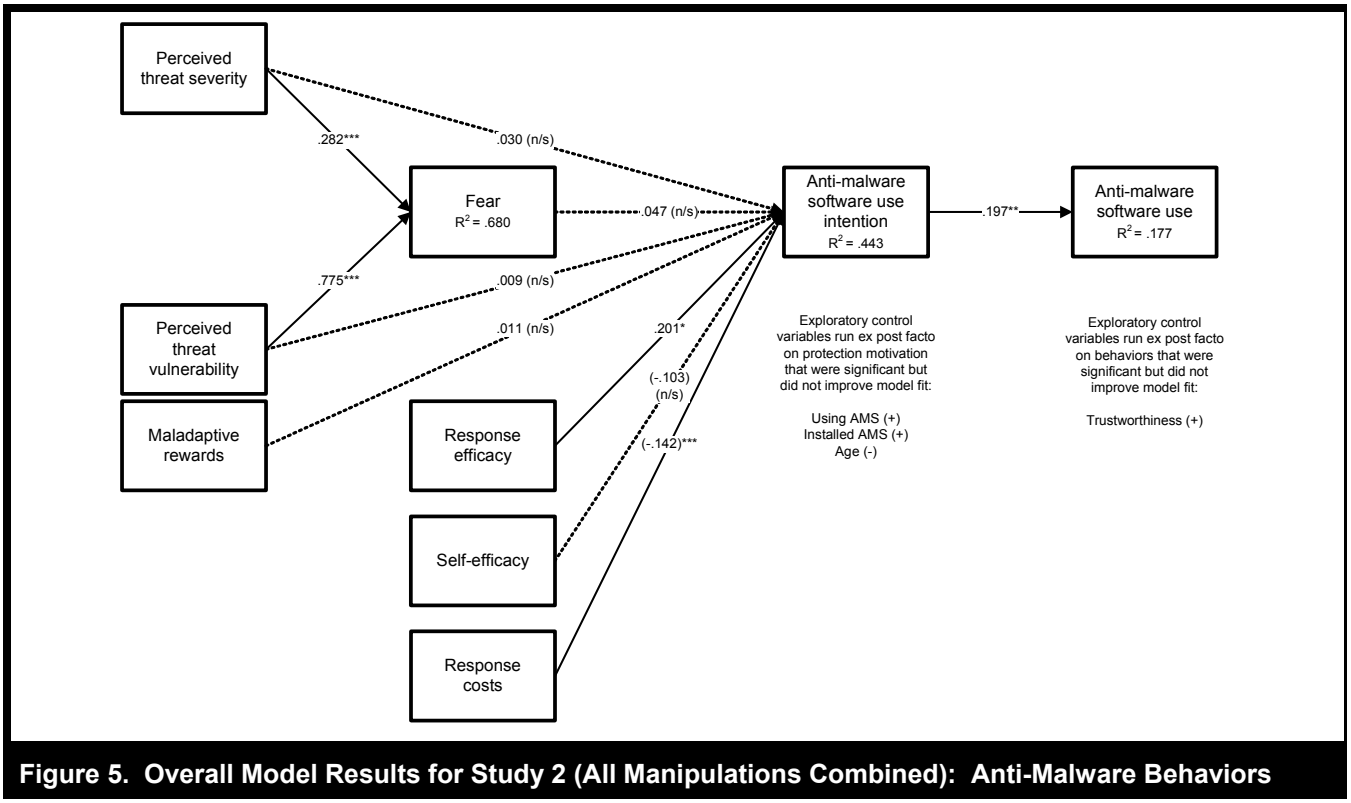

Figure 5. Overall Model Results for Study 2 (All Manipulations Combined): Anti-Malware Behaviors

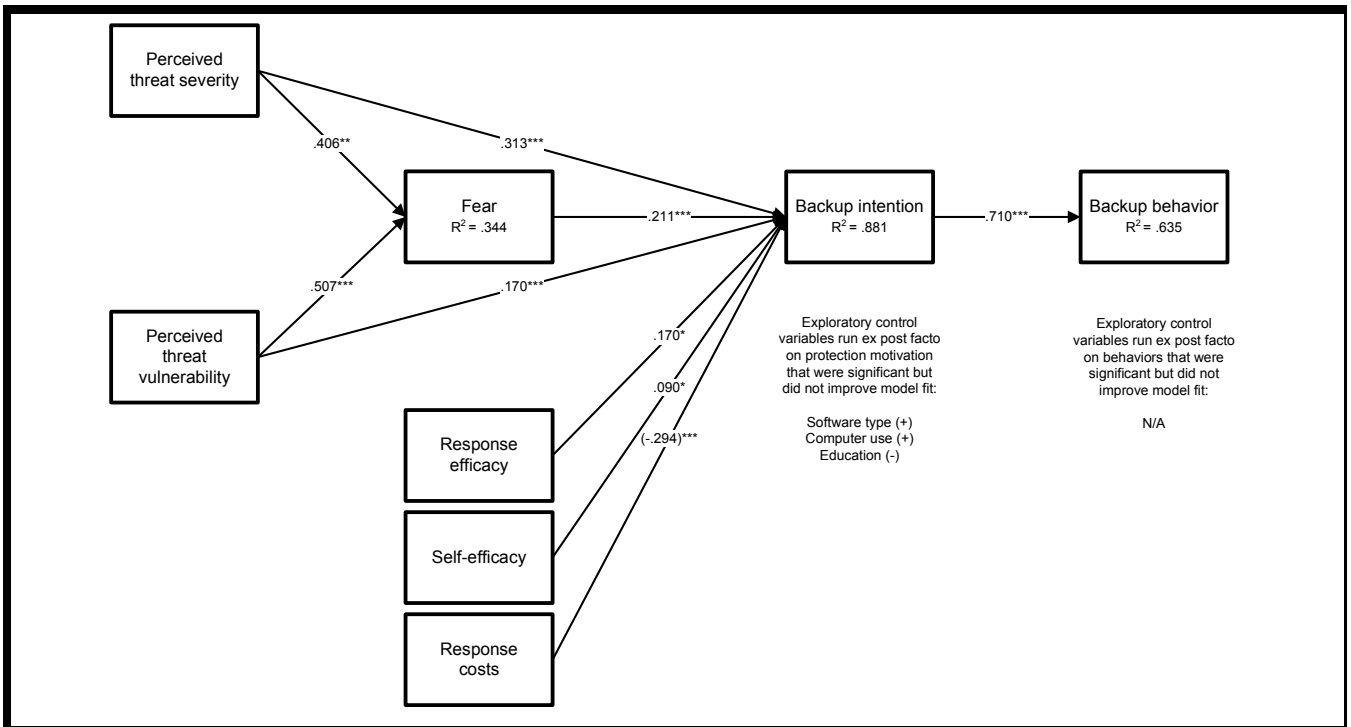

Figure 6. Subsample Results for Study 1: High Fear-Appeal Manipulation

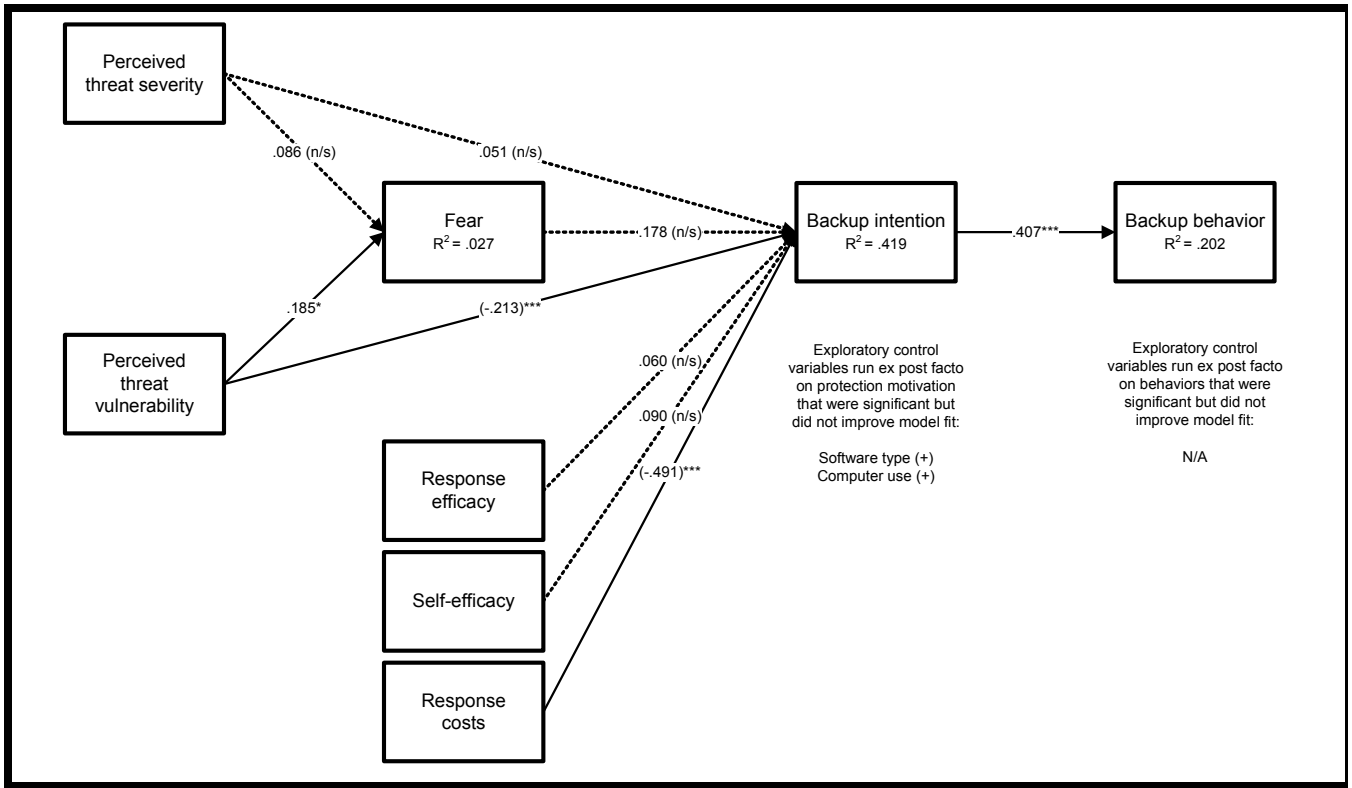

Figure 7. Subsample Results for Study 1: Low Fear-Appeal Manipulation

Study 2 Analysis and Results

The same procedures used in Study 1 were used in Study 2 to assess the data prior to the analysis of the entire model. Convergent and discriminant validities were assessed with confirmatory factor analysis. Model fit was acceptable (χ^2_{2107} = 6067.02; CFI = 0.948; TLI = 0.935; RMSEA = 0.045; CD = 1.000). Convergent validity was supported by large and standardized loadings for all constructs ($p < .001$) and t-values that exceeded statistical significance. Convergent validity was also supported by calculating the ratio of factor loadings to their respective standard errors, which exceeded |10.0| ($p <$ .001).

Discriminant validity was tested by verifying that the measurement model had a better fit than a competing model with a single latent construct and all other competing models in which pairs of latent constructs were joined. The χ^2 differences between the competing models (omitted for brevity) were significantly larger than that of the measurement model, which was also suggested by the factor loadings, modification indices, and residuals (Marsh and Hocevar 1985). These tests confirmed convergent and discriminant validity.

Reliability was assessed using the composite factor reliability score. All measures exceeded 0.70, suggesting adequate reliability for all constructs. Reliability was also supported in that the average variance extracted (Hair et al. 2006) exceeded 0.70 for all factors. Table 5 summarizes the reliabilities, means, standard deviation, and correlations of Study 2.

Study 2 Model Results

Figures 8 and 9 depict the two subsample models according to fear-appeal level. Fit indices revealed acceptable fit for each model (high fear appeal: χ^2_{2120} = 5729.01; CFI = 0.940; TLI = 0.938; RMSEA = 0.062; CD = 1.000; low fear appeal: χ^2_{2121} = 6175.93; χ^2/df = 2.91; CFI = 0.949; TLI = 0.933; RMSEA = 0.062; CD = 1.000). Again, the R^2 for the high model was much higher than that of the low model, especially in terms of predicting actual behavior.

The full PMT nomology, including fear, played the expected role in the high model, but like Study 1, contradicted PMT in several respects in the low model (e.g., fear backfired by decreasing protection motivation, threat dropped out of the model, and the role of self-efficacy became negative).

Table 5. Study 2 Overall Reliabilities, Means, Standard Deviations, and Correlations

Construct	Rel.	Mean	SD	1	2	3	4	5	6	7
1. Severity	.915	4.16	1.22							
2. Vulnerability	.817	3.99	1.18	0.292						
3. Maladaptive rewards	.777	3.65	1.21	0.080	0.176					
4. Fear	.755	2.88	1.10	0.428	0.542	0.211				
5. Self-efficacy	.929	4.86	1.18	0.084	0.017	-0.258	-0.131			
6. Response efficacy	.898	5.12	1.09	0.213	0.221	-0.178	-0.061	0.579		
7. Response cost	.845	3.64	1.15	0.186	0.227	0.556	0.313	-0.369	-0.126	
8. Intent	.984	5.28	1.73	0.160	0.220	-0.266	0.013	0.341	0.399	-0.217

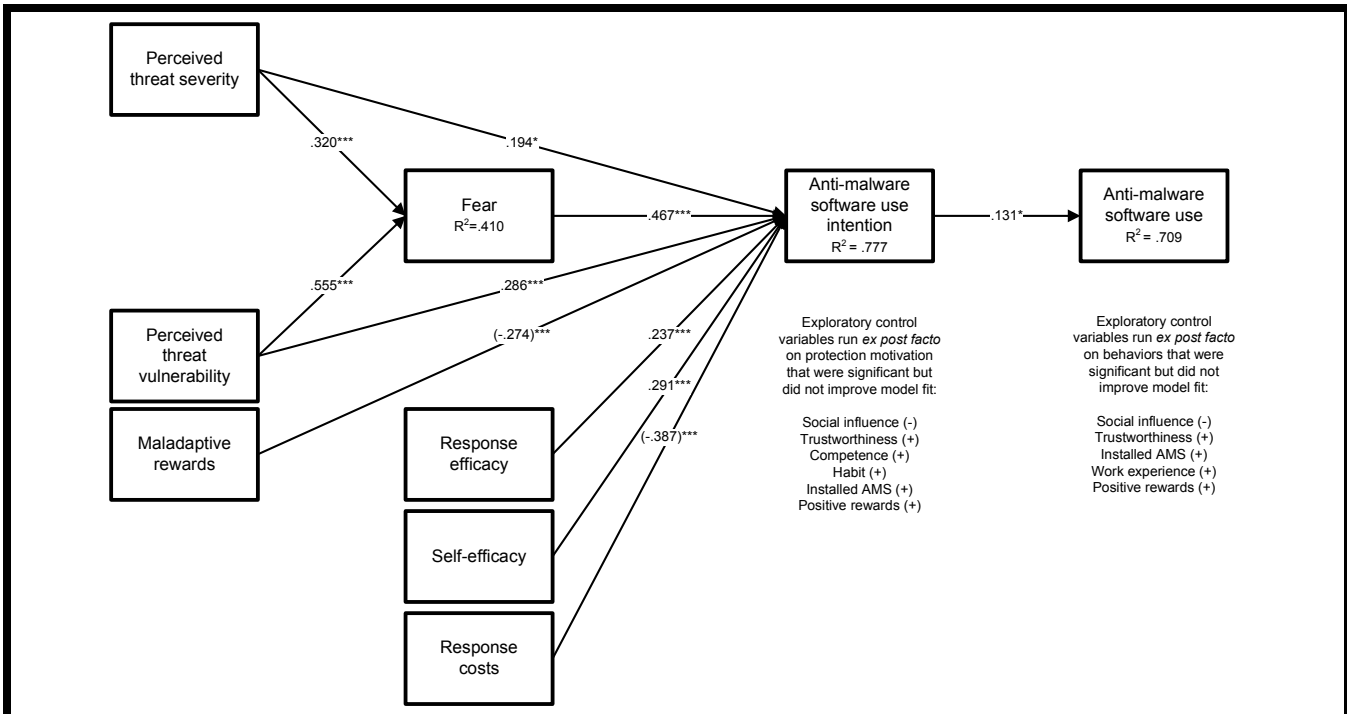

Figure 8. Submodel Results for Study 2: High Fear Appeal for Anti-Malware

Post Hoc Analysis of Extant PMT-Based Models in ISec Research

Given our review of PMT in the ISec context, we now analyze these existing models with our data in an effort to compare the efficacy of our proposed model with the previously described models. This analysis allows us to test more accurately the veracity of our claims regarding the most appropriate nomological implementation of PMT in ISec research by comparing model fit. That is, we show what *would have happened* with *our data* and fear-appeal manipulations in terms of model fit and explained variance had we used a PMT spinoff model as our theoretical foundation rather than the core or full PMT nomologies. We used the larger dataset from Study 2 to analyze the models presented by Lee et al. (2008), Lee and Larsen (2009), Liang and Xue (2010), and Johnston and Warkentin (2010a). We also considered the Herath and Rao (2009) and Johnston et al. (2015) models; however, because of the former's inclusion of policy attitude, and the latter's inclusion of deterrence (they tested their 2010 model without social influence but added deterrence constructs, and yet still had low intentions R^2 results), we could not fully replicate their new additions; thus, they are excluded from this *post hoc* analysis.

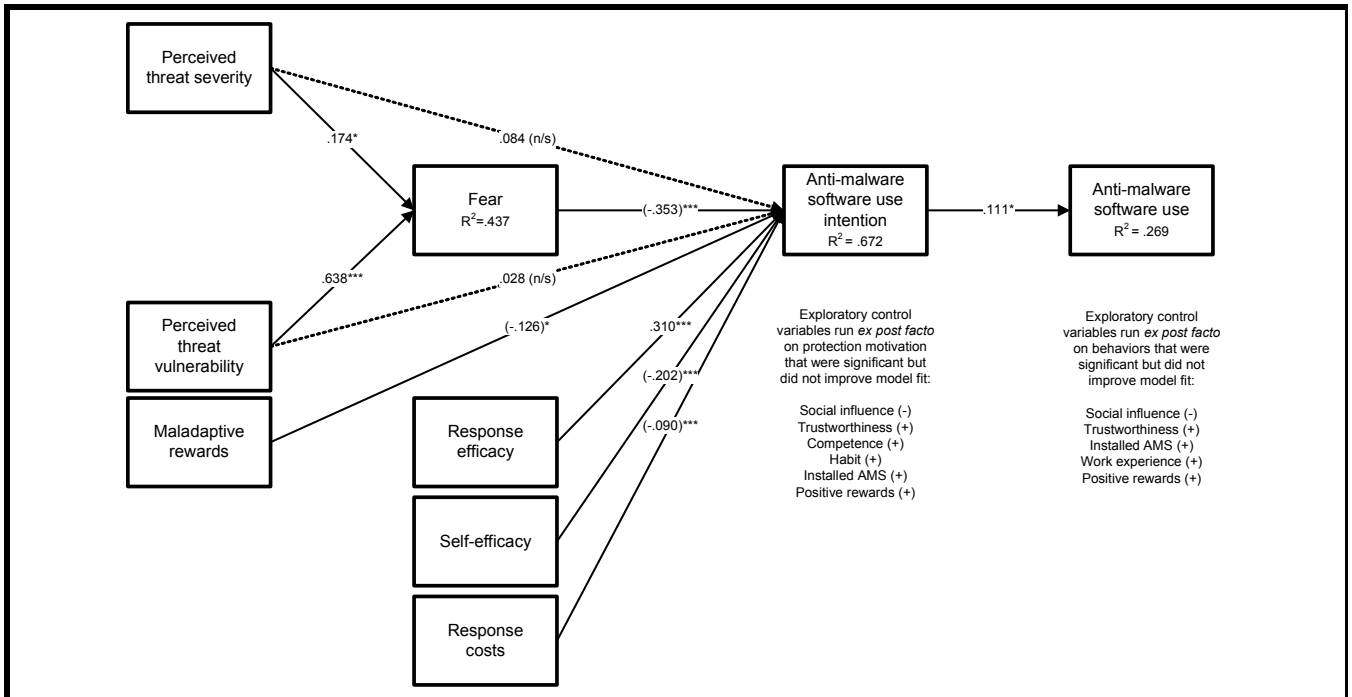

Figure 9. Submodel Results for Study 2: Low Fear Appeal for Anti-Malware

Finally, one other study was excluded from this *post hoc* analysis: that of Marett et al. (2011), whose context was social networking sites. This study is particularly problematic to replicate as it mixes elements of PMT with maladaptive responses (i.e., avoidance and helplessness) found in the extended parallel process model (e.g., Witte 1992, 1994). They correctly thought of many elements of PMT; however, they used one-item measures for several key variables in the model, their fear appeal only involved increasing threat, not efficacy, and all of their responses were regressed together, without considering differences in fear-appeal manipulations. Not surprisingly, they found support only for two protection motivation antecedents (intrinsic rewards and threat severity), and no support for antecedents to coping-appraisal (self-efficacy, response efficacy, and response costs).

We used the same data-validation and model-fit checks as we did in the previous two studies; however, for the sake of brevity and to focus on the more relevant issue of comparing the fit indices of different models, we included only outcomes of the analysis using our best PMT-compliant data: the high manipulations from Study 2. Importantly, just as with our model when using all of the data (both high and low manipulations), all of these models suffered from generally lower model fit, lower R^2, and fewer supported paths when using all of the data. Table 6 summarizes these tested models against the full PMT nomology, including model-fit statistics.

When reviewing Table 6, it is useful to compare the numbers from the previous studies against the examination of our full model (described as Study 2c), which includes some experimental non-PMT covariates. The statistics for the prior studies are from *their* complete models as well, using our data, some of which include non-PMT constructs, and some of which exclude some PMT constructs. Therefore, we believe the most useful comparison is between the statistics in the final column against the statistics from the other studies using our data. All include the high fear-appeal data points only.

Lee et al. (2008) proposed a main-effects model wherein all elements of PMT were directly related to the intentions to protect oneself from a threat. We replicated this model, as shown on the left side of Figure 10. Notably, they added "prior experience" from outside PMT, and omitted testing the following relationships and constructs: severity → fear; vulnerability → fear; fear → protection motivation; and protection motivation → behavior.

Lee and Larsen (2009) next proposed a similar model that included behaviors and social influence (outside of PMT) while controlling for aspects of the organization (vendor support, IT budget, and firm size). We replicated the PMT portion of the model without similar control variables and removed behavior because the other models lacked behavior; this is also why we excluded the relationship between inten-

Table 6. Summary of Model-Fit Statistics Using Only Our "High" Manipulation Fear-Appeal Data from Study 2 Applied to Key Previous Models

Statistic/Path	Desired level	Lee et al. (2008)	Lee and Larsen (2009)	Liang and Xue (2010)*	Johnston and Warkentin (2010a)	Study 2a Core	Study 2b Full	Study 2c Complete
CFI	> .90	.870	.903	.398	.906	.841	.940	.948
TLI	> .90	.854	.890	.344	.887	.823	.938	.935
RMSEA	< .08	.096	.090	.301	.103	.101	.062	.045
Final R^2	N/A	.453	.258	.247	.170	.249	.419	.777
Aside from model-fit considerations, the following relationships should be supported if PMT holds:								
Severity → Fear	Yes	Missing	Missing	Missing	Missing	Yes	Yes	Yes
Vulnerability → Fear	Yes	Missing	Missing	Missing	Missing	Yes	Yes	Yes
Severity → PM	Yes	No	No	No	Missing	Yes	Yes	Yes
Vulnerability → PM	Yes	No	Yes	No	Missing	Yes	Yes	Yes
Fear → PM	Yes	Missing	Missing	Missing	Missing	n/a	Yes	Yes
Maladaptive → PM	Yes	No	Missing	Missing	Missing	n/a	Yes	Yes
Response efficiency → PM	Yes	No	No	No	No	Yes	Yes	Yes
Self-efficiency → PM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Costs → PM	Yes	No	Yes	Yes	Missing	Yes	Yes	Yes
PM → Behavior	Yes	Missing	Yes	Missing	Missing	Yes	Yes	Yes

*Not a full replication, as noted in the text (we did not use a second-order threat construct as they did). Greyed cells represent undesirable model-fit statistics or required PMT paths that are not significant; Study 2a models our high only Study 2 data against the core PMT nomology that omits fear and maladaptive rewards so that we can demonstrate that the full PMT demonstrates superior model fit and R^2; Study 2b is the same data against the full PMT nomology with no added covariates; Study 2c is the full nomology with our added exploratory covariates. The associated acceptable-level fit statistics guidelines are from Gefen et al. (2011).

tion and behavior. They omitted testing the following relationships and constructs: severity → fear; vulnerability → fear; fear → protection motivation; and maladaptive rewards → protection motivation.

The technology threat avoidance theory (Liang and Xue 2010), included the same constructs as PMT, but the authors proposed interactions between severity and vulnerability in predicting a threat and then added an interaction between perceived threat and response efficacy to predict protection motivation. We replicated this model without the inclusion of a second-order perceived threat. We could not measure perceived threat with its own items, and it became unmanageable to predict a second-order construct with its main effects and an interaction construct through methods that would allow for the measurement of the first-order constructs (severity and vulnerability) using the latent construct score or a repeated indicator approach. Rather, we placed the relationships from severity and vulnerability as well as their interaction directly onto protection motivation. Importantly they omitted testing the following PMT relationships: severity → fear; vulnerability → fear; fear → protection motivation; maladaptive rewards → protection motivation; protection motivation → behavior. Figure 11 shows the results of the analysis of this model. Their proposed interaction terms caused serious model-fit issues.

Finally, we replicated the model developed by Johnston and Warkentin (2010a) in Figure 12. In this model, they proposed that the two types of efficacy in PMT are impacted by the levels of perceived severity and vulnerability. Notably, they omitted testing the following PMT relationships: severity → fear; vulnerability → fear; severity → protection motivation; fear → protection motivations; maladaptive rewards → protection motivations; response costs → protection motivation; protection motivation behavior.

In summary, this comparison between applying our data to existing models demonstrates the best model-fit indices for the full PMT model that we advocate in this paper. We also show that the model proposed in this study has greater predictive power regarding protection motivation intentions than any other model. These results further make a dramatic case for (1) using the full PMT nomology, (2) using manipulated fear-appeals, (3) following PMT's assumption that it is only designed for highly personally relevant threat and fear, along with strong coping responses through efficacy—not for all possible manipulations such as low threat.

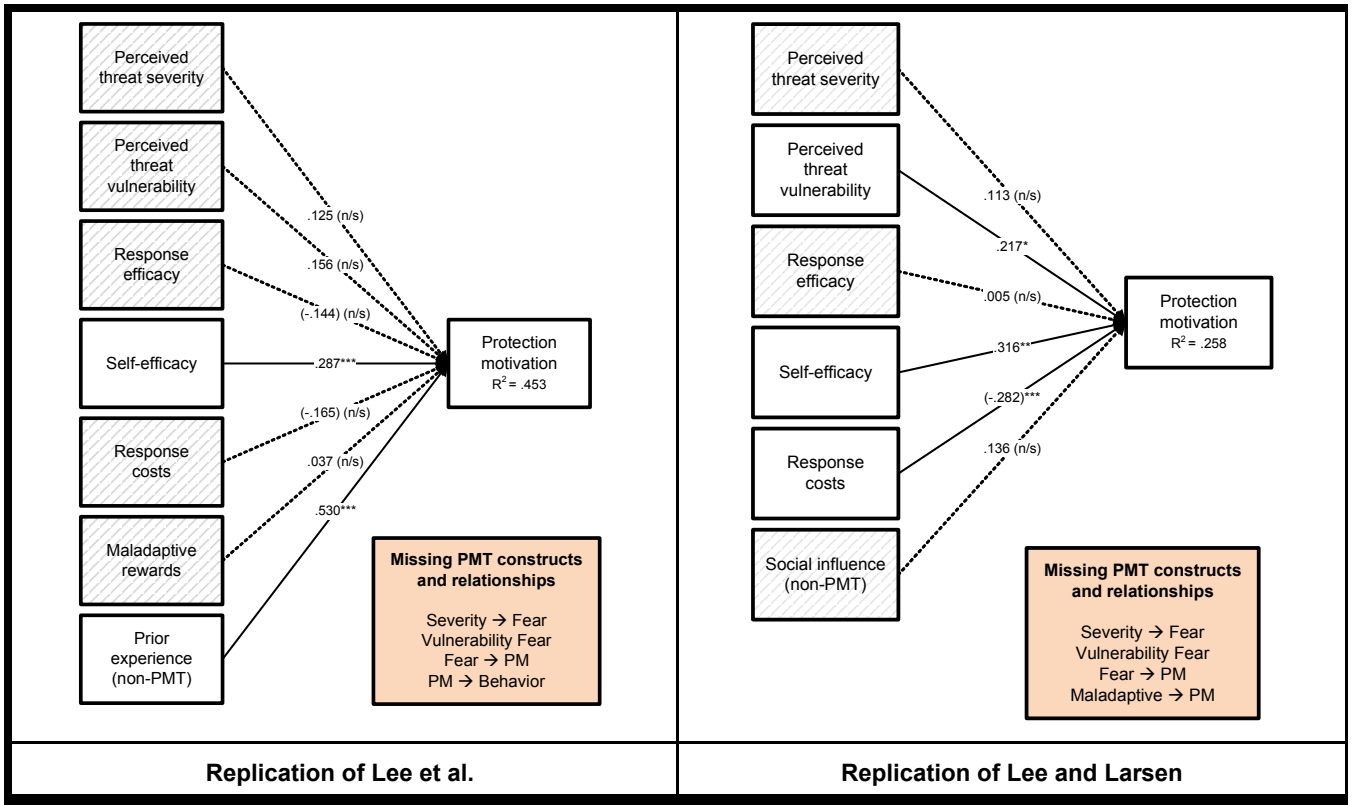

Figure 10. Results for the Lee et al. (2008) and Lee and Larsen (2009) Models Using Only the High Manipulation Study 2 Data*

*Unsupported relationships are further denoted with checked constructs; Lee et al. added "prior experience" outside of PMT; Lee and Larsen added "social influence" outside of PMT but they did test behavior.

Discussion

The purpose of this article was to review PMT-based ISec studies and demonstrate how they could benefit from closer adherence to the nomology and assumptions of PMT. In reviewing the ISec PMT literature, we discovered the four theoretical and methodological opportunities that motivated this article:

1. Incomplete treatment of the core and full nomology of constructs in PMT
2. Omission of fear-appeal manipulations
3. Omission of fear measurement
4. Failure to measure actual protective behaviors

To demonstrate that these are, indeed, areas that can be readily addressed by ISec researchers to improve PMT research, we tested PMT in two different ISec context that closely model the modern theoretical treatment of PMT. In both studies, we included manipulated fear appeals as well as intentions (i.e., protection motivation) and actual protective behaviors. Notably, a recent article by Posey et al. (2013) pointed to a key limitation of the frequent reliance of ISec research on only one behavioral context in which to test a model. Posey et al. noted that this practice inhibits theory development and has the practical limitation of inhibiting "researchers' understanding of insiders' ability to perform multiple protective behaviors" (p. 1190). Thus, our use of two different PMT contexts contributes to both theory and practice.

Study 1 used a longitudinal approach using the context of data backups. Participants who were e-mailed three fear appeals over the course of a semester reported significantly higher fear and stronger intentions to perform backups, and they conducted more actual backups. Actual automated logs from participants with backup software closely matched the self-report measures in the backup logs. We further discovered that the perceived costs associated with backing up data were

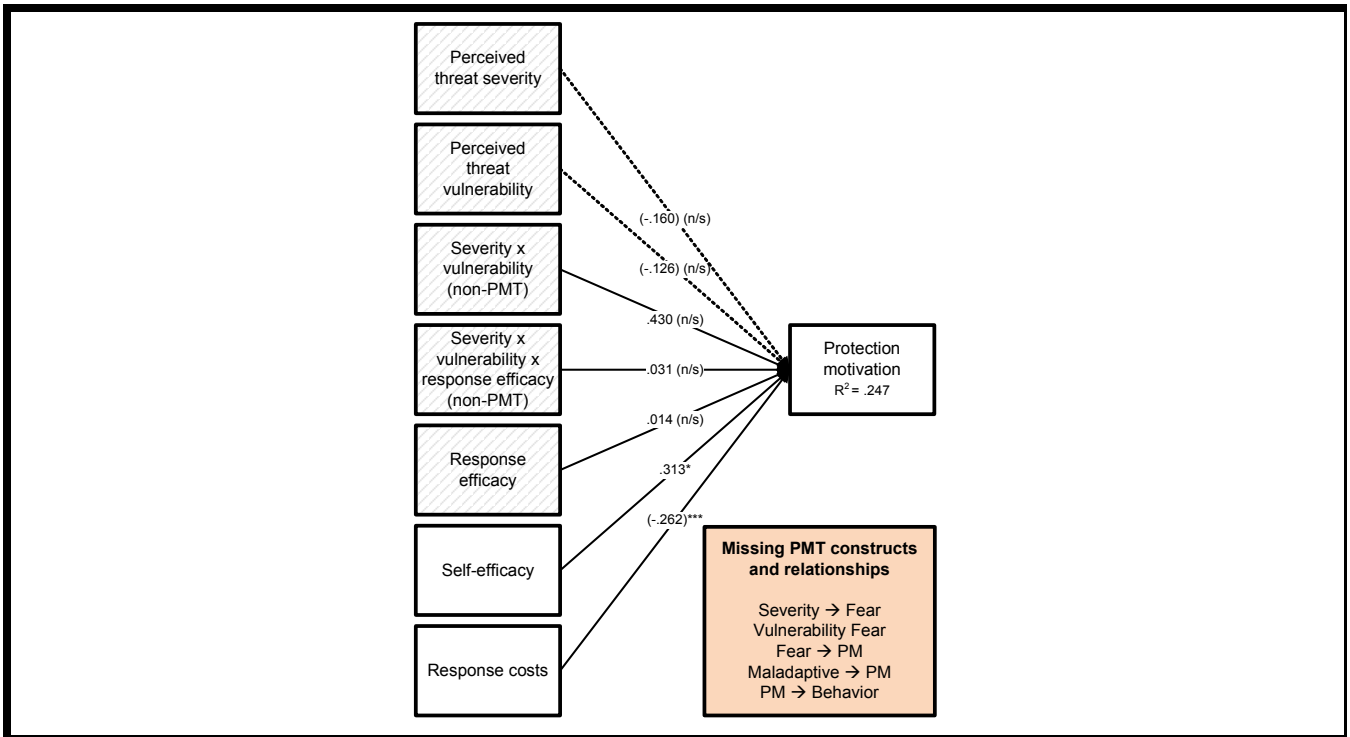

Figure 11. Results for the Liang and Xue (2010 Model Using Only the High Manipulation Study 2 Data*

*As noted in the text, this is not a perfect replication as we did not use a second-order threat construct as did Liang and Xue as this is not core to PMT.

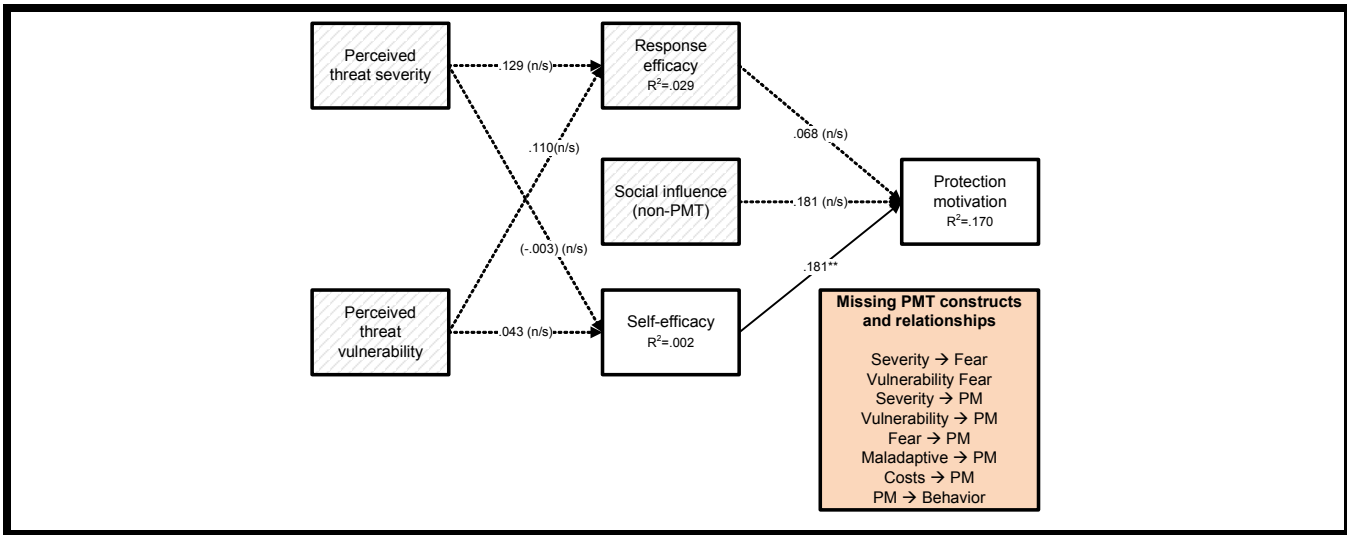

Figure 12. Results for the Johnston and Warkentin (2010a) Model Using Only the High Manipulation Study 2 Data

the most important predictor of backup intentions. Of greater importance, when a strong fear-appeal manipulation was used, the core PMT model was fully supported, along with the core assumptions of PMT; however, when a weak fear-appeal manipulation as used, the PMT model did not hold: threat severity was not significant, fear dropped out of the model, threat vulnerability incorrectly decreased protection motivation, both self-efficacy and response efficacy dropped out, and the R^2 values for both protection motivation and behavior dropped dramatically.

Study 2 applied PMT in a short-term cross-sectional domain that also had a strong and weak fear-appeal manipulation. Participants who received the strong fear appeal exhibited results similar to those of Study 1: higher levels of fear, stronger behavioral intentions, and more actual protective behavior. Although the path coefficients between the strong and weak manipulations had greater similarities than in Study 1, the treatments produced pronounced effects and markedly increased the significance levels of all pathways. We again found that response costs were an important predictor of protective intentions, but in this context, fear exhibited increased significance as the most important predictor. As in Study 1, when a fear-appeal manipulation was used in Study 2, the full PMT model was fully supported (including maladaptive rewards), along with the core assumptions of PMT; however, when a weak fear-appeal manipulation was used, the PMT model did not hold: threat severity and threat vulnerability were insignificant, and both fear and self-efficacy reversed themselves and became negative factors in the relationship with protection motivation (contrary to PMT).

Contributions to Research and Theory

Having established the efficacy of our more complete use of PMT, we now explain our contributions to research and theory in the context of the research opportunities that guided this project. We also provide recommendations for research and theory related to these opportunities.

Recommendation #1: ISec PMT researchers should ideally use and establish the core or full nomology of PMT before adding non-PMT constructs.

We demonstrated that using either the core or full nomology of PMT is crucial to a faithful appropriation of PMT and that extant modifications in the literature that exclude portions of PMT are more likely to end up with weaker theoretical and empirical model fit than models using the full nomology. Most previous ISec studies omitted maladaptive rewards for noncompliance (as did Study 1). Every study omitted fear. FAM, a truncated version of PMT that adds social influence, also omitted response costs and model paths not shown in PMT. The model developed by Lee and Larsen (2009) also added social influence without a complete PMT nomology. Moreover, TTAT (Liang and Xue 2010)—again, not claimed by the authors to be a PMT model, but often incorrectly cited as such—added multiplicative relationships that were predicted in an earlier version of PMT (Rogers 1983) and that were later discredited and removed from PMT.

A lesson from our research is that before ISec researchers expand or truncate PMT, they need to demonstrate that their new use of PMT is a theoretical and empirical improvement on the intended use and modeling of PMT. For example, before adding social influence, researchers need to test the full nomology of PMT with proper model-fit statistics, which are available only via covariance-based SEM—notably not via PLS, which lacks these statistics and is more appropriate for preliminary model development, not for testing well-established nomologies (Lowry and Gaskin 2014)—and then test the addition of social influence. Otherwise, it will be impossible to ascertain whether the addition of the construct is an improvement to PMT or actually degrades model fit. This is especially crucial for a theory as well established as PMT, which has been examined in hundreds of studies.

Recommendation #2: ISec PMT researchers should ideally use fear-appeal manipulations when conducting security-related PMT studies.

These interesting results from Studies 1 and 2 emphasize the conclusion we drew from our literature review on PMT: proper fear-appeal manipulations are a core assumption of proper PMT use. We showed that high fear-appeal manipulations produce more fear and supporting threat that inspires protection motivation than do low fear-appeal manipulations. We also showed that models with higher fear appeals create stronger results than those with lower fear appeals, especially when it comes to influencing actual behaviors. If the fear-appeal message does not cause an individual to perceive fear, then that individual will be less likely to protect him- or herself from the threat, because it is not seen as dangerous. Consequently, not using fear-appeal manipulations violates PMT and causes potentially spurious and misleading results that undermine the established PMT nomology. Using a weak fear appeal will introduce needless, unexplained variation in a PMT model.

The widespread absence of fear appeals might thus be the most problematic omission in the ISec literature, because it is the contextual basis upon which PMT is built. A fear appeal is more than simply an ISec policy, a manual, a code of ethics, or knowledge of a threat, because these are typically not designed to directly address and manipulate threat severity,

threat vulnerability, maladaptive rewards, self-efficacy, response efficacy, or response costs.

Moreover, as demonstrated in our literature review, the purpose of a fear appeal is to generate a threat and level of fear sufficient to motivate a change in behavior. Our empirical results clearly demonstrate the utility of a fear appeal and the ability to separate those who have been made afraid by a strong appeal from those exposed to a weak appeal. Previous ISec research has proposed theoretical models wherein those with and without fear-appeal manipulations are maintained in one model. Our results and analysis indicate that such models may be convoluting the results by not recognizing the key differences among effective threat appraisal and coping appraisal, and ineffective threat appraisal and coping appraisal, which are core assumptions of PMT. In modeling recipients of strong and weak fear appeals separately, we find, in congruence with tenets of PMT, that only high fear-appeal participants properly engaged in threat appraisal in an adaptive manner—thus processing a useful level of fear and threat that also kicked off a useful coping-appraisal process (using self-efficacy, response efficacy, and response costs). In the weak fear-appeal groups, not only was the threat-appraisal process undermined, but the coping-appraisal process was as well, and in both cases the result was much lower protection motivation and subsequent behavior.

Recommendation #3: ISec PMT researchers should measure fear when conducting security-related PMT studies.

We also provided theoretical and empirical evidence that fear should be measured for three key reasons:

(1) Fear is shown to be a core partial mediator in the most recent established revision of PMT (Floyd et al. 2000; Rogers and Prentice-Dunn 1997); both Study 1 and Study 2 show the same partial mediation, indicating that the ISec PMT nomology is thus likely incomplete without fear.

(2) Furthermore, threat is not equivalent to fear; thus, evaluating the efficacy of a fear appeal without measuring fear itself is problematic (LaTour and Rotfeld 1997; Witte 1992, 1994; Witte and Allen 2000).

(3) Fear is easily recalled, described, and measured through established perceptual survey methods drawn from psychology and fear-appeals research, including self-reporting (Osman et al. 1994; Scherer 2005; Witte 1992).

We demonstrate such effective self-reported measurement even in our longitudinal setting. Thus, one cannot fully ascertain the effectiveness of a fear appeal simply by examining the threat and ignoring the measurement of fear. Different levels of fear should be generated by different levels of fear appeals. Hence, providing fear-appeal manipulations and measuring the resulting fear are core assumptions in the use of PMT.

Recommendation #4: ISec PMT researchers should ideally model and measure behaviors, not only intentions.

Extant ISec PMT studies have focused on security-related intentions and ignored actual behavioral change. Although PMT is an intentions-focused model, it has been effectively extended to behaviors (Floyd et al. 2000). Actual behaviors are important for ISec research because the end goal is to change security behaviors, not just security intentions. By measuring both the intentions and actual behaviors, we were able to show that the path from intentions to actual behavior is more pronounced in the high fear-appeal conditions in both of our studies, which demonstrates the importance of using real fear appeals and not just security policies or general threats. This higher level of fear indicates that organizations should provide strong messages about the consequences of risky situations and ways to avoid potentially damaging and pervasive behavioral security weaknesses.

An additional methodological benefit of measuring actual behaviors in addition to self-reported intentions and other measures is that such an approach greatly decreases the possibility of common-method biases by combining two methods for collecting data. Studies that focus solely on self-report, as is the case with the ISec PMT literature, are subject to greater threats from common-method bias (Podsakoff et al. 2003).

In summary, by building on the foundation of previous ISec PMT studies, we have demonstrated practical ways in which researchers can improve PMT-related studies, while taking into account PMT's hybrid nature as partly a variance model and partly a process model, per Burton-Jones et al. (2015). Researchers will also be able to approach their studies with less confusion about how to model PMT; they will be able to remedy important limitations in the published ISec literature and to avoid truncated or unexpectedly altered models, omission of fear appeals, and failure to observe actual behavior. Researchers will also be aware of the similar applicability of our proposed model to both longitudinal and short-term experimental studies in the context of users who should back up their data as well as act on warnings from antivirus software. Finally, researchers will have a baseline model to draw upon to extend PMT properly to other variables such as social influence or company policy.

Implications for Practice

Practitioners should note that a fear appeal is more than the existence of an ISec policy, a manual, a code of ethics, the knowledge of a threat, or merely scaring people; the existence of a statement that opposes insecure behavior is not necessarily persuasive, nor does it necessarily invoke fear. A fear appeal requires a persuasive message that ideally is designed to heighten threat severity and vulnerability sufficiently to generate fear and to help address maladaptive incentives to ignore the fear appeal. The fear appeal should likewise address issues that can increase self-efficacy and response efficacy while decreasing response costs. Hence, in practice, fear appeals typically require campaigns, interventions, and training. To increase their effectiveness, multiple applications over time are required. In summary, an effective fear appeal generally inspires an adaptive approach to both threat appraisal and coping appraisal, resulting in an adaptive, protective response rather than message rejection.

Our research should provide practitioners with evidence for the need to use fear appeals and to present users with strong arguments for adhering to behavioral security policies. Users who do not appreciate the consequences of maladaptive behavior are a perennial problem in organizations worldwide. Response costs and maladaptive benefits should be minimized so users do not find it appealing to ignore a well-intentioned, well-reasoned policy and/or warning that describes a behavioral security danger.

Limitations and Future Research

As with any study, there are some caveats that need to be considered when interpreting our results and conducting future research. First, we used student participants for both studies, although in each context, the task appeared appropriate for students, and the two samples represented two different age groups with highly similar results: graduate MBA students in Study 1 and undergraduate students taking a psychology class in Study 2. The similarity of results demonstrates a relative insensitivity to age and discipline, although more research needs to be performed with even older participants or those in other occupations for greater assurance of the invariability of results. Moving beyond this baseline, other security-related tasks that may or may not be appropriate for students need to be investigated.

A second limitation is the use of only two contexts in the studies: data backups and the use of anti-malware software. Future research will need to examine other contexts of behavioral security to further establish the efficacy of PMT-based research and identify additional areas for improvement. For example, it remains to be seen how our suggested improvements to PMT research will be able to improve ISec policy compliance in general, as opposed to more focused behaviors. Finally, it is difficult to know the extent to which experimental realism was maintained. However, given that our data could be easily applied to other ISec PMT models, our comparison holds any potential artifacts constant and compares the models themselves.

Another important limitation of this study is inherent within the assumptions of PMT. First, PMT largely ignores emotions other than fear. PMT is based primarily on rational thought processes and intentional thinking, which makes it similar to the theory of reasoned action (Fishbein and Ajzen 1975) and the theory of planned behavior (Ajzen 1991). Moreover, although PMT includes fear, it assumes that people respond rationally to fear by protecting themselves. However, as noted by Leventhal (1970), even though emotional coping mechanisms may also be evident, this possibility is excluded from PMT. Second, current applications of PMT effectively explain the processes and outcomes of danger control, but they have been mostly silent on the processes and outcomes of fear control. Therefore, future research should explore the possible dual outcomes by considering the dual-process routes afforded by the dual-process model (Leventhal 1970) or by the more recent extended parallel process model (Witte 1992, 1994; Witte and Allen 2000). For example, future research could explore antecedents for why individuals fail to behave in a secure manner.

A fourth limitation of this study deals with the application of the fear appeal as a moderating influence in our model. As we discussed, based on McClendon and Prentice-Dunn (2001), there are three possible approaches to treating stronger and weaker fear appeals in a theoretical model. The first, using fear appeal as an antecedent of the model, was not supported by the literature. The second, modeling the fear appeal as a moderator for each of the nine links, was mathematically infeasible, especially when using CB-SEM software. Although a PLS approach might be feasible, the absence of model fit statistics and the lack of error variance at the construct level could overstate the significance of the relationships.

Finally, although we have made a compelling case for a renewed emphasis on fear appeals, fear, and the PMT nomology in ISec research, we do not claim to have addressed every issue related to these concepts. Their absence in the previous literature points to a need for further methodological and theoretical research to refine fear appeals and fear measurement for ISec. For one, creating ideal fear appeals is not easy, because they should be built in view of the threat (severity and vulnerability) and in view of efficacy (self-

efficacy and response efficacy), and they need to be generalizable to a wide target audience to create an appropriate level of fear. Also, as demonstrated by Johnston et al. (2015), they need to have personal relevance. Thus, more work is needed to establish guidelines on how to inspire the right level of fear and to explain better what happens if too much fear is generated. It is also likely that there are behavioral security situations for which PMT and fear appeals simply are not appropriate and for which other theoretical approaches may be better. Our strong fear appeals represent a good start, but certainly more can be done to ensure that adaptive threat-appraisal and coping-appraisal responses are generated with fear appeals in various ISec contexts and to better consider ways to also increase efficacy as part of fear appeals.

For example, although we have followed standard psychological practices on the self-reporting of fear, we acknowledge the suggestion by Crossler et al. (2013) that the ideal fear measure might be one that is applied at the moment of occurrence. This is best achieved under tight experimental controls (e.g., fMRI, EKG, or galvanic skin response). Creating a realistic fear measurement of ISec behaviors under such conditions is thus highly complex and could be the "holy grail" of this line of research. The advantage of such a measure would be to reduce further the possibility of common-method bias (Podsakoff et al. 2003), as we did in measuring actual behaviors. However, measuring physiological fear is much more complicated than measuring actual behaviors. It might be necessary to use slightly less invasive techniques, such as eye tracking (e.g., Twyman et al. 2015), examining mouse movements (e.g., Hibbeln et al. 2014), recording keystroke delay (e.g., Jenkins et al. 2013), or leveraging a wearable galvanic skin response measurement device (e.g., Moody and Galletta 2015), and to collect such data under deceptive conditions so that participants do not know that fear- and threat-response measures are the key study focus. Longitudinal data collection would also be beneficial for this approach, especially for ongoing fear-appeal campaigns through security education training and awareness (SETA) initiatives.

We also expect that there are key differences in longitudinal and one-time fear-appeal studies that require further theoretical and methodological study. The effects of fear differed somewhat between the two studies (although fear played a partial mediating role, as expected, in both studies), and we attribute this to the difference between a strong and focused one-time fear-appeal message and one that is made somewhat weaker by the longitudinal nature of the manipulation. In Study 2, individuals were presented with a very sudden, unexpected, and potentially catastrophic fear appeal threatening that all of their data might be lost within the next reboot cycle of the computer. This potentially had a greater impact on protection motivations and behaviors, because the safety of actual data was perceived to be at stake. In Study 1, however, messaging was about the potential of data loss at some point, and the study never presented the participants with definitive messaging about its imminent loss. ISec researchers might find it unrealistic to measure maladaptive rewards if the behavior is not focused on a single moment or decision (e.g., Study 1). Future researchers might ask participants in longitudinal field studies to recall their fear or perceptions of maladaptive responses after the study's completion as a surrogate for assessment during the study. Such measurement can be particularly valuable in cases in which fear appeals differ greatly in effectiveness or in which individual differences lead participants to perceive them differentially. We thus believe that the timing of fear appeals and of fear measurement and the design and process of fear-appeal delivery are highly relevant to the IT artifact delivery, design, and process in ISec studies. We leave it to future research to expand and improve on this vast area of opportunity in IT artifact-related fear appeals.

References

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

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

Burton-Jones, A., McLean, E., and Monod, E. 2015. "Theoretical Perspectives in IS Research: From Variance and Process to Conceptual Latitude and Conceptual Fit," *European Journal of Information Systems* (forthcoming).

Claar, C. L., and Johnson, J. 2012. "Analyzing Home PC Security Adoption Behavior," *Journal of Computer Information Systems* (52:4), pp. 20-29.

Crossler, R. E., and Bélanger, F. 2014. "An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument," *DATA BASE for Advances in Information Systems* (45:4), pp. 51-71.

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

de Hoog, N., Stroebe, W., and de Wit, J. B. F. 2007. "The Impact of Vulnerability to and Severity of a Health Risk on Processing and Acceptance of Fear-Arousing Communications: A Meta-Analysis," *Review of General Psychology* (11:3), pp. 258-285.

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*, Reading, MA: Addison-Wesley.

Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. 2000. "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology* (30:2), pp. 407-429.

Fry, R. B., and Prentice-Dunn, S. 2005. "The Effects of Coping Information and Value Affirmation on Responses to a Perceived Health Threat," *Health Communication* (17:2), pp. 133-147.

Fry, R. B., and Prentice-Dunn, S. 2006. "Effects of a Psychosocial Intervention on Breast Self-Examination Attitudes and Behaviors," *Health Education Research* (21:2), pp. 287-295.

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

Hair, Jr., J. F., Black, W. C., Babin, B. J., and Anderson, R. E. 2006. *Multivariate Data Analysis* (7th ed.), New York: Prentice Hall.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., and Rao, H. R. 2012. "Security Services as Coping Mechanisms: An Investigation into User Intention to Adopt an Email Authentication Service," *Information Systems Journal* (24:1), pp. 61-84.

Herath, T., and Rao, H. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Hibbeln, M., Jenkins, J., Schneider, C., Valacich, J., and Weinmann, M. 2014. "Investigating the Effect of Insurance Fraud on Mouse Usage in Human-Computer Interactions," in *Proceedings of the 35th International Conference on Information Systems,* Auckland, New Zealand, December 14-17.

Hovland, C. I., Janis, I. L., and Kelley, H. H. 1953. *Communication and Persuasion*, New Haven, CT: Yale University Press.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?," *Communications of the ACM* (54:6), pp. 54-60.

Jenkins, J. L., Grimes, M., Proudfoot, J., and 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 Warnings," *Information Technology for Development* (20:2), pp. 196-213.

Johnston, A. C., and Warkentin, M. 2010a. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:1), pp. 549-566.

Johnston, A. C., and Warkentin, M. 2010b. "The Influence of Perceived Source Credibility on End User Attitudes and Intentions to Comply with Recommended IT Actions," *Journal of Organizational and End User Computing* (22:3), pp. 1-21.

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

LaTour, M. S., and Rotfeld, H. J. 1997. "There Are Threats and (Maybe) Fear-Caused Arousal: Theory and Confusions of Appeals to Fear and Fear Arousal Itself," *Journal of Advertising* (26:3), pp. 45-59.

Lee, D., Larose, R., and Rifon, N. 2008. "Keeping Our Network Safe: A Model of Online Protection Behaviour," *Behaviour & Information Technology* (27:5), pp. 445-454.

Lee, Y., and 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), pp. 177-187.

Leventhal, H. 1970. "Findings and Theory in the Study of Fear Communications," in *Advances in Experimental Social Psychology,* L. Berkowitz (ed.), New York: Academic Press, pp. 119-186.

Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11:7), pp. 394-413.

Lowry, P. B., and Gaskin, J. 2014. "Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose it and How to Use it," *IEEE Transactions on Professional Communication* (57:2), pp. 123-146.

Lowry, P. B., and Moody, G. D. 2015. "Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organizational Information Security Policies," *Information Systems Journal* (25:5), pp. 433-453.

Lowry, P. B., Posey, C., Bennett, R. J., and Roberts, T. L. 2015. "Leveraging Fairness and Reactance Theories to Deter Reactive Computer Abuse Following Enhanced Organisational Information Security Policies: An Empirical Study of the Influence of Counterfactual Reasoning and Organisational Trust," *Information Systems Journal* (25:3), pp. 193-273.

Maddux, J. E., and 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), pp. 469-479.

Marett, K., McNab, A. L., and 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), pp. 170-188.

Markus, M. L., and Robey, D. 1988. "Information Technology and Organizational-Change: Causal-Structure in Theory and Research," *Management Science* (34:5), pp. 583-598.

Marsh, H. W., and Hocevar, D. 1985. "Application of Confirmatory Factor Analysis to the Study of Self-Concept: First- and Higher Order Factors Models and Their Invariance across Groups," *Psychological Bulletin* (97:3), pp. 562-582.

McClendon, B. T., and Prentice-Dunn, S. 2001. "Reducing Skin Cancer Risk: An Intervention Based on Protection Motivation Theory," *Journal of Health Psychology* (6:3), pp. 321-328.

McIntosh, D. N., Zajonc, R. B., Vig, P. S., and Emerick, S. W. 1997. "Facial Movement, Breathing, Temperature, and Affect: Implications of the Vascular Theory of Emotional Efference," *Cognition & Emotion* (11:2), pp. 171-195.

Milne, S., Orbell, S., and Sheeran, P. 2002. "Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and Implementation Intentions," *British Journal of Health Psychology* (7), pp. 163-184.

Milne, S., Sheeran, P., and Orbell, S. 2000. "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory," *Journal of Applied Social Psychology* (30:1), pp. 106-143.

Moody, G. D., and Galletta, D. F. 2015. "Lost in Cyberspace: The Impact of Information Scent and Time Constraints on Stress, Performance, and Attitudes," *Journal of Management Information Systems* (forthcoming).

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

Osman, A., Barrious, F. X., Osman, J. R., Schneekloth, R., and Troutman, J. A. 1994. "The Pain Anxiety Symptoms Scale: Psychometric Properties in a Community Sample," *Journal of Behavioral Medicine* (17:5), pp. 511-522.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.

Posey, C., Roberts, T. L., Bennett, R., and Lowry, P. B. 2011. "When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse," *Journal of Information System Security* (7:1), pp. 24-47.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS Quarterly* (37:4), pp. 1189-1210.

Rippetoe, P. A., and 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), pp. 596-604.

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

Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in *Social Psychophysiology: A Sourcebook,* J. T. Cacioppo, and R. E. Petty (eds.), New York: Guilford, pp. 153-176.

Rogers, R. W., and Prentice-Dunn, S. 1997. "Protection Motivation Theory," in *Handbook of Health Behavior Research I: Personal and Social Determinants,* D. S. Gochman (ed.), New York: Plenum Press, pp. 113-132.

Scherer, K. R. 2005. "What Are Emotions? And How Can They Be Measured?," *Social Science Information* (44:4), pp. 695-729.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2008. "Process Variance Models in Information Security Awareness Research," *Information Management & Computer Security* (16:3), pp. 271-287.

Twyman, N. W., Lowry, O. B., Burgoon, J. K., and Nunamaker, J. F. 2015. "Autonomous Scientifically Controlled Screening Systems for Detecting Information Purposely Concealed by Individuals," *Journal of Management Information Systems* (31:3), pp. 106-137.

Vance, A., Lowry, P. B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263-289.

Vance, A., Lowry, P. B., and Eggett, D. 2015. "Increasing Accountability Through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations," *MIS Quarterly* (39:2), pp. 345-366.

Wall, J. D., Palvia, P., and Lowry, P. B. 2013. "Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy," *Journal of Information Privacy and Security* (9:4), pp. 52-79.

Witte, K. 1992. "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," *Communication Monographs* (59:4), pp. 329-349.

Witte, K. 1994. "Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM)," *Communication Monographs* (61:2), pp. 113-134.

Witte, K. 1998. "Fear as Motivator, Fear as Inhibitor: Using the Extended Parallel Processing Model to Explain Fear Appeal Successes and Failures," in *Handbook of Communication and Emotion: Research, Theory, Application, and Contexts,* P. A. Anderson, and L. K. Guerrero (eds.), San Diego, CA: Academic Press, pp. 423-450.

Witte, K., and Allen, M. 2000. "A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns," *Health Education & Behavior* (27:5), pp. 591-615.

Witte, K., Cameron, A., McKeon, J. K., and Berkowitz, J. M. 1996. "Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale," *Journal of Health Communication* (1:4), pp. 317-342.

About the Authors

Scott R. Boss joined the Bentley University Department of Accountancy after receiving his Ph.D. in Information Systems from the University of Pittsburgh in 2007. His research concentrates on information security, controls, cybercrime, and fraud. His work has been published in *European Journal of Information Systems*, *Group and Organization Management*, International Journal of *Accounting Information Systems*, and *Business Process Management Journal*. He is one of the founding members of the IFIP WG8.11/ WG11.13 Dewald Rood International Workshop on IS Security Research. Scott teaches classes on advanced accounting information systems and fraud in the graduate school at Bentley University.

Dennis F. Galletta (Ph.D., University of Minnesota) is an AIS Fellow, serving as a professor and Doctoral Program Director at the Katz Business School, University of Pittsburgh. He has published in journals such as *MIS Quarterly*, *Management Science*, *Information Systems Research*, *Journal of Management Information Systems*, *European Journal of Information Systems*, and *Journal of the AIS*, and has served on the editorial boards of *MIS Quarterly*, *Journal of Management Information Systems*, *Information Systems Research*, and *Journal of the AIS*. In 2006, he received the *MIS Quarterly* "Developmental Associate Editor" award. Dennis has served as both program and general conference chair/co-chair for the International Conference on Information Systems and the Americas Conference on Information Systems, and has co-chaired the ICIS Doctoral Consortium. He served as ICIS Treasurer, AIS President,

and AIS Council Member. He is one of the founding Editors-in-Chief of *AIS Transactions on HCI* and established the concept of AIS Special Interest Groups in 2000.

Paul Benjamin Lowry is a professor of Information Systems at the Department of Information Systems, City University of Hong Kong. He received his Ph.D. in Management Information Systems from the University of Arizona and an MBA from the Marriott School of Management. He has published over 70 journal articles in *MIS Quarterly*, *Information System Research*, *Journal of Management Information Systems*, *Journal of the AIS*, *Information Systems Journal*, *European Journal of Information Systems*, and many others. He currently serves as a senior editor for *Decision Sciences* and *AIS Transactions on HCI*, and as an associate editor for *European Journal of Information Systems*, *Information & Management*, *Communications of the AIS*, and *Information Security Education Journal*. He has also served as a track chair for conferences including ICIS, ECIS, and PACIS. His research interests include organizational and behavioral security/privacy issues, HCI and decision sciences, e-commerce and supply chains, and scientometrics.

Gregory D. Moody holds two doctorates in Information Systems from the University of Pittsburgh and the University of Oulu. He is currently an assistant professor at the University of Nevada, Las Vegas. Greg has published in journals including *MIS Quarterly*, *Journal of Management Information Systems*, *Information Systems Journal*, *Journal of the AIS*, and *Communications of the AIS*. His interests include IS security and privacy, e-business (electronic markets, trust) and human–computer interaction (Web site browsing, entertainment). He is currently an associate editor for *Information Systems Journal* and *AIS Transactions on Human–Computer Interactions*, and an officer in SIGHCI.

Peter Polak is a lecturer at Florida International University. He holds a Ph.D. from the University of Pittsburgh in MIS. His research interests include human–computer interaction, internet technologies, and human factors. He has published in *Information Systems Research*, *Journal of the AIS*, *Communications of the ACM*, and *International Journal of Human–Computer Interaction*, among others. His teaching revolves around web application development, programming, databases, and network security, which he has taught in the United States, Egypt, and the Netherlands.

MIS Quarterly

WHAT DO SYSTEMS USERS HAVE TO FEAR? USING FEAR APPEALS TO ENGENDER THREATS AND FEAR THAT MOTIVATE PROTECTIVE SECURITY BEHAVIORS

Scott R. Boss
Department of Accountancy, Bentley University, 175 Forest Street,
Waltham, MA 02452 U.S.A. {sboss@bentley.edu}

Dennis F. Galletta
Katz Graduate School of Business, University of Pittsburgh, 282a Mervis Hall,
Pittsburgh, PA 15260 U.S.A. {galletta@katz.pitt.edu}

Paul Benjamin Lowry
College of Business, City University of Hong Kong, P7718, Academic 1,
Hong Kong, CHINA {Paul.Lowry.PhD@gmail.com}

Gregory D. Moody
University of Nevada, Las Vegas, 329 Frank and Estella Beam Hall, 4515 S. Maryland Parkway, Mail Stop 6034,
Las Vegas, NV 89154 U.S.A. {gregory.moody@unlv.edu}

Peter Polak
Department of Decision Sciences & Information Systems, College of Business, Florida International University,
11200 S.W. 8th St., RB 250, Miami, FL 33199 U.S.A. {ppolak@fiu.edu}

Appendix A

Reviewed PMT-Related Journal Articles

Table A1. Overview of All ISec Journal Articles that Use Portions of PMT

Citation, journal (field)	Context (behaviors studied)	Constructs of core PMT missing from their study	Constructs of full PMT missing from their study	Non-PMT constructs added without testing the full PMT nomology first	Other choices not consistent with PMT (and theories added without confirming PMT first)
Anderson and Agarwal (2010) MISQ (field: IS)	Practicing safe computing at home (intentions to practice secure behaviors)	• Threat severity • Threat vulnerability • Response costs	• Maladaptive rewards • Fear	• Public goods • Psychological ownership • Subjective norm • Descriptive norms	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Added theory: public goods and psychological ownership
Claar and Johnson (2012) JCIS (field: IS)	Home PC security (self-report use of home security)	• Protection motivation • Response efficacy • Response costs (partial)	• Maladaptive rewards • Fear	• Benefits • Cues to action	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Reworked response costs as perceived barriers • Added theory: health belief model
Crossler and Bélanger (2014) DATA BASE (field: IS)	Students' security behaviors (multiple security behaviors)	N/A	• Maladaptive rewards • Fear	N/A	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics
Foth et al. (2012) JPH (field: Health)	Hospital employees' data-protection compliance (reported intention to comply)	Response efficacy Self-efficacy Response costs	• Maladaptive rewards • Fear	• Subjective norm • Data-protection level • Perceived usefulness • Perceived ease of use • Attitude	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Used data-protection level to subsume severity of and vulnerability to threat • Added theory: TAM (attempt was to merge PMT and TAM)
Gurung et al. (2009) IMCS (field: security)	Students' motivations to use antispyware (self-reported use of antispyware software)	• Protection motivation • Response costs	• Maladaptive rewards • Fear	N/A	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics
Herath and Rao (2009b) EJIS (field: IS)	Employees' ISP compliance (ISP compliance intentions)	N/A	• Maladaptive rewards • Fear	• Punishment severity • Detection certainty • Security-breach concern • Attitude • Subjective norm • Descriptive norm • Resource availability • Organizational commitment	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Added theory: apparent attempt at a unified model by mixing parts of PMT, GDT, TPB, DTPB, and organizational commitment
Herath et al. (2012) ISJ (field: IS)	User intentions to adopt e-mail authentication (intention to adopt authentication)	• Threat severity • Threat vulnerability • Response efficacy • Protection motivation	• Maladaptive rewards • Fear	• Threat appraisal • Overall appraisal of external coping • Usefulness • Perceived ease of use • Responsiveness • Privacy concern • Privacy notification practice • Adoption intention	• Contrary to PMT, used a combined construct of threat appraisal like EPPM • Contrary to PMT, used a combined construct of coping appraisal like EPPM • No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Added theory: TTAT and TAM (attempt was to merge PMT, TTAT, and TAM)

Table A1. Overview of All ISec Journal Articles that Use Portions of PMT (Continued)

Citation, journal (field)	Context (behaviors studied)	Constructs of core PMT missing from their study	Constructs of full PMT missing from their study	Non-PMT constructs added without testing the full PMT nomology first	Other choices not consistent with PMT (and theories added without confirming PMT first)
Ifinedo (2012) C&S (field: security)	Understanding ISP compliance of employees (intentions to comply to ISPs)	N/A	• Maladaptive rewards • Fear	• Subjective norms • Perceived behavioral control	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Added theory: TPB
Jenkins et al. (2013) ITD (field: IS)	Students' creation of unique passwords (observed passwords)	• Protection motivation • Response costs	• Maladaptive rewards • Fear	N/A	• No model-fit statistics • No path model; PMT as a secondary application for a manipulation check of the experiment
Johnston and Warkentin (2010a) MISQ (field: IS)	Employees' and students' intentions to follow recommended actions to avert spyware (intentions to avert spyware)	• Response costs	• Maladaptive rewards • Fear	• Social influence	• No model-fit statistics • Called their model "fear appeals model (FAM)" although used PMT for core concepts • Contrary to PMT and EPPM, modeled threat severity and vulnerability directly to response efficacy and self-efficacy
Lai et al. (2012) DSS (field: decision science)	Students' coping with identity theft (self-report of identity theft)	• Threat severity • Threat vulnerability • Response efficacy • Response costs	• Maladaptive rewards • Fear	• Technological coping • Conventional coping • Identity theft • Perceived effectiveness	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics (although they used LISREL) • Appeared to conceptualize response efficacy as perceived effectiveness, although not quite the same • DV was a maladaptive outcome (ID theft) • Added theory: TTAT (primary a TTAT study but not true to TTAT)
LaRose et al. (2008) CACM (field: computing)	Online safety of employees (intentions to be safe)	• Response costs	• Maladaptive rewards • Fear	• Ease of use • Perceived usefulness • Relative advantage • Attitude toward behavior • Image • Visibility • Trialability • Involvement • Social norm • Personal responsibility • Moral compatibility • Habit • Perceived behavioral control	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Added theory: ELM, social cognitive theory, TAM • Not testable and not repeatable, because it summarizes multiple studies but does not provide adequate detail on the model, measurement, method, and statistics
Lee et al. (2008) BIT (field: HCI)	Encouraging students to use virus protection (virus-protection intention)	• Response costs	• Maladaptive rewards • Fear	• Positive outcome expectations • Negative outcome expectations • Prior virus infection	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Added theory: SCT
Lee and Larsen (2009) EJIS (field: IS)	Executives' decisions to adopt anti-malware software	• Response efficacy • Self-efficacy	• Maladaptive rewards • Fear	• Social influence • Vendor support • IT budget • Firm size	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics

Table A1. Overview of All ISec Journal Articles that Use Portions of PMT (Continued)

Citation, journal (field)	Context (behaviors studied)	Constructs of core PMT missing from their study	Constructs of full PMT missing from their study	Non-PMT constructs added without testing the full PMT nomology first	Other choices not consistent with PMT (and theories added without confirming PMT first)
Lee (2011) DSS (field: IS)	Faculty members' adoption of antiplagiarism software (intentions and self-report behaviors)	N/A	• Maladaptive rewards • Fear	• Moral obligation • Social influence	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Added theory: Oddly, paper was framed as an EPPM study, but it theoretically fits PMT better than EPPM because it used constructs like PMT, not EPPM (e.g., no combined threat, no combined efficacy, no maladaptive outcome path and constructs).
Liang and Xue (2010) JAIS (field: IS)	Antispyware intentions and behaviors in students' computer use (intentions and behaviors associated with antispyware use)	N/A	• Maladaptive rewards • Fear	N/A	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Renames "response efficacy" as "safeguard effectiveness"; "response cost" as "safeguard cost"; "protection motivation" as "avoidance motivation" • Creates a second-order construct of "perceived threat," which is congruous with EPPM, not PMT • Proposes an old interaction effect between severity and vulnerability further increasing "perceived threat," which is not supported by PMT findings • Proposes an interaction between perceived threat and response efficacy, which has also not been supported in the literature • Added theory: called their model "TTAT" although used PMT constructs as a core component of their model
Marett et al. (2011) AIS-THCI (field: IS/HCI)	Students' threat to privacy on social networking sites (intentions toward privacy behaviors)	• Threat vulnerability	• Maladaptive rewards (incorrect conceptualization) • Fear (one-measure, wrong relationship)	• Avoidance • Hopelessness	• Used concepts from EPPM and incorrectly attributed them to PMT • Made PMT into a parallel process model like EPPM • No model-fit statistics • Maladaptive rewards incorrectly conceptualized • Fear had incorrect relationship in model for PMT; used as a one-item nonvalidated manipulation check • Used one-item measures for response efficacy, response costs, fear, and intention
Milne et al. (2009) JCA (field: consumer behavior)	Consumers' risky behavior and protection practices (self-report adaptive and maladaptive behaviors)	• Response costs • Response efficacy • Protection motivation	• Maladaptive rewards • Fear	• Maladaptive behaviors	• Added maladaptive outcomes to model, changing it to a parallel-process model like EPPM, not PMT (yet, ignored maladaptive rewards) • No fear appeals • No IV manipulation; static model using survey • No model-fit statistics
Mohamed and Ahmad (2012) CHB (field: HCI)	Students' protection behaviors on social media sites (self-report behaviors)	• Protection motivation • Response costs	• Fear	• Information privacy concerns	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics
Ng et al. (2009) DSS (field: IS)	Employees' secure e-mail behavior (self-report behaviors)	• Protection motivation • Response costs (partial) • Response efficacy	• Fear	• Cues to action • General security orientation • Perceived barriers	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Response costs are partially covered by "perceived barriers" • Severity was reconceptualized as a moderator of every relationship in the model • Added theory: Study is based on a derivation of the health belief model, derived from PMT.

Table A1. Overview of All ISec Journal Articles that Use Portions of PMT (Continued)

Citation, journal (field)	Context (behaviors studied)	Constructs of core PMT missing from their study	Constructs of full PMT missing from their study	Non-PMT constructs added without testing the full PMT nomology first	Other choices not consistent with PMT (and theories added without confirming PMT first)
Salleh et al. (2012) JISN&VC (field: social computing)	Students' self-disclosure behavior on social networking sites (self-report of self-disclosure)	• Protection motivation • Response costs	• Fear	• Privacy concern • Perceived risk • Trust • Information disclosure	• Rather than an adaptive outcome, focused on maladaptive outcome (i.e., information disclosure) • Used "perceived benefits" for maladaptive rewards • No fear appeals • No IV manipulation; static model using survey • No model-fit statistics
Siponen et al. (2010) IEEEC (field: computing)	Employees' motivation to comply with ISPs (intentions and self-reported behaviors)	• Threat severity • Threat vulnerability • Response costs	• Maladaptive rewards • Fear	• Normative beliefs • Visibility • Deterrence	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Added theory: GDT, TRA, innovation diffusion theory • Incorrectly fused threat constructs similar to EPPM
Vance and Siponen (2012) JOEUC (field: IS/HCI)	Employees' ISP compliance (intentions to comply)	N/A	• Maladaptive rewards • Fear	• Habit	• No fear appeals • No IV manipulation; static model using survey • No model-fit statistics • Incorrectly bundled rewards as one construct • Added theory: habit theory
Workman (2009) IM&CS (field: security)	Explaining employees' security lapses at work (security-lapse behaviors)	• Protection motivation	• Maladaptive rewards • Fear	• Trust • Process transparency • Inherent fairness • Adjudication process • Attitude	• No fear appeals • No manipulation; static • No model-fit statistics • Added theory: psychological contract theory and justice theory
Yoon et al. (2012) JISE (field: IS)	Explaining students' secure behaviors (intentions and self-report behaviors)	N/A	• Maladaptive rewards • Fear	• Subjective norm • Security habits	• No fear appeals • No manipulation; static • No model-fit statistics • Added theory: TPB
Zhang and McDowell (2009) JIC (field: e-commerce)	Students' use of strong passwords (intentions to use strong passwords)	• Self-efficacy	• Fear	N/A	• No fear appeals • No manipulation; static • No model-fit statistics • This article oddly added fear but dropped self-efficacy and maladaptive rewards
Study 1 (this paper)	Students' use of backup software to protect themselves (intentions and observed behaviors)	N/A	• Maladaptive rewards	N/A	• Maladaptive rewards likely would change over time, and in a longitudinal study, might be impractical to measure
Study 2 (this paper)	Students' use of anti-malware software to protect themselves (intentions and observed behaviors)	N/A	N/A	N/A	N/A

Explanation of PMT Spinoff Models

A key issue revealed by our review is that several ISec articles are cited by others as PMT studies when in fact they involve new models that are inspired by PMT but are actually positioned as alternative models to PMT. We believe it is better to refer to these as *PMT spinoffs* that use some PMT constructs. The key issue with all of hese studies, however, is that although they are not testing PMT per se, they have created alternative models inspired by PMT without demonstrating that they have better explanatory power or model fit than PMT. If this trend

continues, it will become impossible to know which model ISec researchers and practitioners should be using. To clarify this common misunderstanding, we explicitly review four types of alternative models to PMT: (1) the technology threat avoidance theory (TTAT) model, as proposed by Liang and Xue (2010); (2) the fear-appeals model (FAM) proposed by (Johnston and Warkentin 2010); (3) extensions to the health-belief model (HBM) by Ng et al. (2009) and Claar and Johnson (2012); (4) and various efforts to create "unified" models that merge parts of PMT with other theories, such as those developed by Herath and Rao (2009a) and Herath et al. (2012).

PMT Spinoff Model Type 1: The Technology Threat Avoidance Theory (TTAT)

The technology threat avoidance theory (TTAT) model was proposed by Liang and Xue (2010), who stated that they provided partial empirical support for their previous work. They very accurately characterize their model as "complicated" (p. 404) because it includes a process model, a variance model, and many constructs. Their results are valuable because they demonstrate the value of security, education, and awareness programs and indicate directions for further research in the area. However, several papers have exhibited a misunderstanding of their model by citing it as a PMT model.

Notably, the creators of TTAT do not claim to be testing PMT. In fact, they rename some existing PMT constructs with similar names and create some relationships that are actually contrary to the original PMT model. For instance, in TTAT, "response efficacy" becomes "safeguard effectiveness"; "response cost" becomes "safeguard cost"; and "protection motivation" becomes "avoidance motivation." Rather than following PMT's prediction that threat severity and threat vulnerability will directly impact protection motivation, TTAT creates the second-order construct "perceived threat," which follows the extended parallel processing model (EPPM) (Witte and Allen 2000), not PMT. Likewise, TTAT proposes an interaction effect between severity and vulnerability, which further increases "perceived threat" (in H1c). That interaction is actually part of an older version of PMT (Rogers 1975) that is no longer in use because it has not been supported by empirical results and meta-analysis (Floyd et al. 2000; Milne et al. 2000; Rogers and Prentice-Dunn 1997). TTAT also proposes a new interaction between perceived threat and response efficacy (H3a) that has also not been supported in the literature (Floyd et al. 2000; Milne et al. 2000). Finally, TTAT excludes fear or fear appeals from the model and empirical results. Importantly, TTAT has never been directly compared to the core nomology of PMT and its assumptions. Ironically, another study (Lai et al. 2012) that recently built on TTAT made radical deletions and additions to that model (see Table A.1). However, it did not establish itself against the core nomology and assumptions of PMT.

PMT Spinoff Model Type 2: The Fear-Appeals Model (FAM)

The fear-appeals model (FAM) was proposed by Johnston and Warkentin (2010). As with TTAT, several papers incorrectly refer to FAM as a PMT model when the authors did not represent FAM as implementing PMT. FAM provides a new, simplified arrangement of the relationships among the standard PMT constructs and adds social influence as an additional construct. However, FAM also omits response costs, although it uses fear appeals (but does not measure fear). FAM also rearranges the relationships between threat and efficacy by using severity and vulnerability as the direct predictors for response efficacy and self-efficacy, in contradiction to both PMT and EPPM.

PMT Spinoff Model Type 3: The Health Belief Model (HBM)

Several other studies build on the health belief model (HBM), which is a newer derivation of PMT from health communication research, and the derivations raise several concerns in an ISec context. A study by Claar and Johnson (2012) used HBM to explain the use of home security, but omitted protection motivation, response efficacy, maladaptive rewards, and fear. Additionally, the study omitted fear appeals and the response costs construct, and measurement appears to differ significantly from the original definitions in PMT. Another study (Ng et al. 2009) used HBM to explain employees' secure e-mail behavior. This study omitted protection motivation, response efficacy, and fear appeals, and it reconceptualized response costs as "perceived barriers." The study additionally modeled threat severity as an antecedent to every relationship in the model against security behaviors.

PMT Spinoff Model Type 4: Attempts at Unified Models with Portions of PMT

Finally, several studies have attempted to create a unified model that combines PMT with several other theories. Although these studies have done an admirable job of explaining individual behaviors, they have not demonstrated that their models are superior to PMT or any of the other theories from which they borrow; they are simply interesting combinations of parts of various theories intended to maximize prediction. The first such study (Herath and Rao 2009b) combined PMT and GDT, but some of the key assumptions, constructs, and relationships of these two

theories have been shown to be incompatible (Floyd et al. 2000). The study also omitted fear or fear appeals; in adding GDT, it also added parts of TPB, DTPB, and organizational commitment. A more recent unified model (Herath et al. 2012) merged TTAT and TAM. For our purposes, the drawback to this approach is that because the TTAT model did not claim to be a complete PMT model, this study departs more strongly from PMT by omitting threat severity, threat vulnerability, response efficacy, protection motivation, fear, and fear appeals—as was noted in the discussion of TTAT above. It also adds combined assessments of both threat and coping appraisals, which is interestingly similar to EPPM. The model also adds most of the TAM model (omitting enjoyment), and adds the new constructs responsiveness, privacy concern, and privacy notification.

References

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp. 613-643.

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

Claar, C. L., and Johnson, J. 2012. "Analyzing Home PC Security Adoption Behavior," *Journal of Computer Information Systems* (52:4), pp. 20-29.

Crossler, R. E., and Bélanger, F. 2014. "An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument," *DATA BASE for Advances in Information Systems* (45:4), pp. 51-71.

Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. 2000. "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology* (30:2), pp. 407-429.

Foth, M., Schusterschitz, C., and 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), pp. 253-268.

Gurung, A., Luo, X., and Liao, Q. 2009. "Consumer Motivations in Taking Action against Spyware: An Empirical Investigation," *Information Management & Computer Security* (17:3), pp. 276-289.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., and Rao, H. R. 2012. "Security Services as Coping Mechanisms: An Investigation into User Intention to Adopt an Email Authentication Service," *Information Systems Journal* (24:1), pp. 61-84.

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

Herath, T., and Rao, H. 2009b. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 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), pp. 83-95.

Jenkins, J. L., Grimes, M., Proudfoot, J., and 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 Warnings," *Information Technology for Development* (20:2), pp. 196-213.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:1), pp. 549-566.

Lai, F., Li, D., and Hsieh, C.-T. 2012. "Fighting Identity Theft: The Coping Perspective," *Decision Support Systems* (52:2), pp. 353-363.

LaRose, R., Rifon, N. J., and Enbody, R. 2008. "Promoting Personal Responsibility for Internet Safety," *Communications of the ACM* (51:3), pp. 71-76.

Lee, D., Larose, R., and Rifon, N. 2008. "Keeping Our Network Safe: A Model of Online Protection Behaviour," *Behaviour & Information Technology* (27:5), pp. 445-454.

Lee, Y. 2011. "Understanding Anti-Plagiarism Software Adoption: An Extended Protection Motivation Theory Perspective," *Decision Support Systems* (50:2), pp. 361-369.

Lee, Y., and 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), pp. 177-187.

Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11:7), pp. 394-413.

Lowry, P. B., and Gaskin, J. 2014. "Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It," *IEEE Transactions on Professional Communication* (57:2), pp. 123-146.

Lowry, P. B., and Moody, G. D. 2015. "Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organizational Information Security Policies," *Information Systems Journal* (25:5), pp. 433-463.

Marett, K., McNab, A. L., and 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), pp. 170-188.

Milne, G. R., Labrecque, L. I., and Cromer, C. 2009. "Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices," *Journal of Consumer Affairs* (43:3), pp. 449-473.

Milne, S., Sheeran, P., and Orbell, S. 2000. "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory," *Journal of Applied Social Psychology* (30:1), pp. 106-143.

Mohamed, N., and Ahmad, I. H. 2012. "Information Privacy Concerns, Antecedents and Privacy Measure Use in Social Networking Sites: Evidence from Malaysia," *Computers in Human Behavior* (28:6), pp. 2366-2375.

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

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

Rogers, R. W., and Prentice-Dunn, S. 1997. "Protection Motivation Theory," in *Handbook of Health Behavior Research I: Personal and Social Determinants,* D. S. Gochman (ed.), New York: Plenum Press, pp. 113-132.

Salleh, N., Hussein, R., Mohamed, N., Karim, N. S. A., Ahlan, A. R., and Aditiawarman, U. 2012. "Examining Information Disclosure Behavior on Social Network Sites Using Protection Motivation Theory, Trust and Risk," *Journal of Internet Social Networking & Virtual Communities* (http://www.ibimapublishing.com/journals/JISNVC/2012/281869/281869.pdf).

Siponen, M., Pahnila, S., and Mahmood, M. A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *IEEE Computer* (43:2), pp. 64-71.

Son, J.-Y. 2011. "Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies," *Information & Management* (48:7), pp. 296-302.

Vance, A., and Siponen, M. 2012. "IS Security Policy Violations: A Rational Choice Perspective," *Journal of Organizational and End-User Computing* (24:1), pp. 21-41.

Witte, K., and Allen, M. 2000. "A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns," *Health Education & Behavior* (27:5), pp. 591-615.

Workman, M. 2009. "How Perceptions of Justice Affect Security Attitudes: Suggestions for Practitioners and Researchers," *Information Management & Computer Security* (17:4), pp. 341-353.

Yoon, C., Hwang, J.-W., and Kim, R. 2012. "Exploring Factors That Influence Students' Behaviors in Information Security," *Journal of Information Systems Education* (23:4), pp. 407-415.

Zhang, L., and McDowell, W. C. 2009. "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords," *Journal of Internet Commerce* (8:3-4), pp. 180-197.

Appendix B

Measurement Items for Study 1 and Study 2

Table B1. Study 1 Measurement Items

Construct	Code	Items
Perceived severity (Milne et al. 2002)	PS01	If I were to lose data from my hard drive, I would suffer a lot of pain.
	PS02	Losing data would be unlikely to cause me major problems (R).
Vulnerability (Milne et al. 2002)	PV01	I am unlikely to lose data in the future (R).
	PV02	My chances of losing data in the future are.
Fear (Milne et al. 2002)	FEAR01	I am worried about the prospect of losing data from my computer.
	FEAR02	I am frightened about the prospect of losing data from my computer.
	FEAR03	I am anxious about the prospect of losing data from my computer.
	FEAR04	I am scared about the prospect of losing data from my computer.
Response efficacy (Milne et al. 2002)	RE01	Backing up my hard drive is a good way to reduce the risk of losing data.
	RE02	If I were to back up my data at least once a week, I would lessen my chances of data loss
Self-efficacy; modified computer self-efficacy (Compeau and Higgins 1995) modified to our context	CSE01	... if there was no one around to tell me what to do.
	CSE02	... if I had never used a package like it before.
	CSE03	... if I had only the software manuals for reference.
	CSE04	... if I had seen someone else using it before trying it myself.
	CSE05	... if I could call someone for help if I got stuck.
	CSE06	... if someone else helped me get started.
	CSE07	... if I had a lot of time to complete the job for which the software was provided.
	CSE08	... if I had just the built-in help facility for assistance.
	CSE09	... if someone showed me how to do it first.
	CSE10	... if I had used similar packages like this one before to do the job.
Response cost (Milne et al. 2002)	RC01	The benefits of backing up my hard drive at least once a week outweigh the costs (R).
	RC02	I would be discouraged from backing up my data during the next week because it would take too much time.
	RC03	Taking the time to back up my data during the next week would cause me too many problems.
	RC04	I would be discouraged from backing up my data at least once a week because I would feel silly doing so.
Intentions (Milne et al. 2002)	INT01	I intend to back up my hard drive during the next week.
	INT02	I do not wish to back up my data during the next week (R).

All items were measured using 7-point Likert-type scales from 1 = strongly disagree to 7 = strongly agree.
R = reverse-coded item.

Table B2. Study 2 Measurement Items

Construct (Source)	Measurement Items
Intent to use anti-malware software (Johnston and Warkentin 2010)	1. I intend to use anti-malware software in the next three months. 2. I predict I will use anti-malware software in the next three months. 3. I plan to use anti-malware software in the next three months.
Threat severity (Johnston and Warkentin 2010)	1. If my computer were infected by malware, it would be severe. 2. If my computer were infected by malware, it would be serious. 3. If my computer were infected by malware, it would be significant.
Threat vulnerability (Johnston and Warkentin 2010a)	1. My computer is at risk for becoming infected with malware. 2. It is likely that my computer will become infected with malware. 3. It is possible that my computer will become infected with malware.
Response efficacy (Johnston and Warkentin 2010)	1. Anti-malware software works for protection 2. Anti-malware software is effective for protection. 3. When using anti-malware software, a computer is more likely to be protected.
Self-efficacy (Johnston and Warkentin 2010)	1. Anti-malware software is easy to use. 2. Anti-malware software is convenient to use. 3. I am able to use anti-malware software without much effort.
Fear (Osman et al. 1994)	1. My computer has a serious malware problem. 2. My computer might be seriously infected with malware. 3. The amount of malware on my computer is terrifying. 4. I am afraid of malware. 5. My computer might become unusable due to malware. 6. My computer might become slower due to malware.
Maladaptive rewards (Myyry et al. 2009)	1. Not using an anti-malware application saves me time. 2. Not using an anti-malware application saves me money. 3. Not using an anti-malware application keeps me from being confused. 4. Using an anti-malware application would slow down the speed of my access to the Internet. 5. Using an anti-malware application would slow down my computer. 6. Using an anti-malware application would interfere with other programs on my computer. 7. Using an anti-malware application would limit the functionality of my Internet browser.
Response costs (Woon et al. 2005)	1. The cost of finding an anti-malware application decreases the convenience afforded by the application. 2. There is too much work associated with trying to increase computer protection through the use of an anti-malware application. 3. Using an anti-malware application on my computer would require considerable investment of effort other than time. 4. Using an anti-malware application would be time consuming.

Study 1 and Study 2 Control Variables

After running our final model, we conducted exploratory *ex post facto* analysis in both studies using control variables outside the nomologies we were testing. In this approach, the purpose of the control variables is to test further how complete a theoretical model is and thus determine whether there are any exploratory, exogenous factors that might have an impact on the base model for future modeling extensions. Importantly, in such use, the base model is established first, and then these controls are applied as a last step to see if any significant changes occur in model fit. In both our studies, there were a couple of control variables that had significant paths but did not significantly improve model fit. This process provides further evidence that the underlying supported model is the correct theoretical form of the model. Classic controls that we use in this sense that are deliberately atheoretical and commonly used in the corresponding literature in the same manner include *age* (D'Arcy et al. 2009; Herath and Rao 2009; Hu et al. 2011; Johnston and Warkentin 2010; Siponen et al. 2010; Son 2011), *gender* (D'Arcy et al. 2009; Herath and Rao 2009b; Hu et al. 2011; Johnston and Warkentin 2010; Siponen et al. 2010; Son 2011), *work experience* (Johnston and Warkentin 2010a; Siponen et al. 2010), and *computer use* (D'Arcy et al. 2009; Hu et al. 2011).

The same literature also demonstrates the importance of providing control variables to account for any artifacts that arise simply from the methodological decisions and tools used that could inadvertently affect the underlying theoretical model. Again, these are atheoretical, but specific to methodological choices. A key example is that Siponen et al. (2010), Hu et al. (2011), and Lowry et al. (2013) use scenarios to study their security phenomena. Thus, they add a covariate that checks the respondents' perceptions of the realism of the scenarios, because unrealistic scenarios could skew the models' results.

Along these lines, in Study 1 we also considered the backup software type. Given that we found nothing interesting with our control variables in Study 2, we tried more controls in Study 2 that included some possible counter explanations found in related literature outside of PMT, including the habit of using anti-malware software modified from (Vance and Siponen 2012), whether they experienced social influence to use anti-malware software modified from (Johnston and Warkentin 2010), and whether positive rewards were perceived and present (Posey et al. 2011), not just maladaptive rewards. We also added method-specific checks: whether they use/run/have installed anti-malware software on their own PCs, and whether they were doing the experiment on their own PCs or a lab PC. We were also concerned that although our fake anti-malware software was designed to look like the real thing, a savvy user might find it suspicious. That is why we also ran controls on brand recognition (Lowry et al. 2008) and related constructs from source credibility security research: perceived competence and perceived trustworthiness (Johnston and Warkentin 2010) of the software itself. Whereas our control variables were more extensive and interesting in Study 2, and a couple of them were significant, they still did not significantly improve model fit and often made it worse. Again, these ex post facto tests help especially the efficacy of the underlying PMT nomology in both of our contexts. However, these results do not rule out the possibility that PMT can be effectively extended in the future with similar constructs in different ISec contexts or data collection conditions. Hence, our work in no way obviates the need for future exploratory controls.

References

Compeau, D. R., and Higgins, C. A. 1995. "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19:2), pp. 189-211.

D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Herath, T., and Rao, H. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?," *Communications of the ACM* (54:6), pp. 54-60.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:1), pp. 549-566.

Lowry, P. B., Moody, G. D., Galletta, D. F., and Vance, A. 2013. "The Drivers in the Use of Online Whistle-Blowing Reporting Systems," *Journal of Management Information Systems* (30:1), pp. 153-189.

Lowry, P. B., Vance, A., Moody, G., Beckman, B., and Read, A. 2008. "Explaining and Predicting the Impact of Branding Alliances and Web Site Quality on Initial Consumer Trust of E-Commerce Web Sites," *Journal of Management Information Systems* (24:4), pp. 199-224.

Milne, S., Orbell, S., and Sheeran, P. 2002. "Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and Implementation Intentions," *British Journal of Health Psychology* (7:May), pp. 163-184.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18:2), pp. 126-139.

Osman, A., Barrious, F. X., Osman, J. R., Schneekloth, R., and Troutman, J. A. 1994. "The Pain Anxiety Symptoms Scale: Psychometric Properties in a Community Sample," *Journal of Behavioral Medicine* (17:5), pp. 511-522.

Posey, C., Roberts, T. L., and Lowry, P. B. 2011. "Motivating the Insider to Protect Organizational Information Assets: Evidence from Protection Motivation Theory and Rival Explanations," in *Proceedings of the 2011 Dewald Roode Workshop on Information Systems Security Research, IFIP WG 8.11/11/13*, A. Vance (ed.), Blacksburg, VA, September 23-24, pp. 1-51.

Siponen, M., Pahnila, S., and Mahmood, M. A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *IEEE Computer* (43:2), pp. 64-71.

Son, J.-Y. 2011. "Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies," *Information & Management* (48:7), pp. 296-302.

Vance, A., and Siponen, M. 2012. "IS Security Policy Violations: A Rational Choice Perspective," *Journal of Organizational and End-User Computing* (24:1), pp. 21-41.

Woon, I., Tan, G.-W., and Low, R. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," in *Proceedings of the 26th International Conference on Information Systems,* D. Avison, D. Galletta, and J. I. DeGross (eds.), Las Vegas, NV, December 11-14, pp. 367-380.

Appendix C

Key Terms and Concepts in Fear-Appeals Research

Table C1. Key Terms and Concepts in Fear-Appeals Research

Term/Concept	Definition (Citation)
Adaptive behavior	Purposefully choosing a danger-control response in response to a fear appeal and choosing a behavior that protects against the danger raised in the fear appeal (Floyd et al. 2000; Rogers and Prentice-Dunn 1997)
Adaptive coping response	Same as *adaptive behavior*
Benefits of noncompliance	Same as *maladaptive rewards*
Benefits of maladaptive behaviors	Same as *maladaptive rewards*
Coping appraisal	The process of considering one's self-efficacy, response efficacy, and the costs of performing the adaptive behavior or the response advocated for in the fear appeal (Floyd et al. 2000; Rogers and Prentice-Dunn 1997)
Costs of adaptive behavior	Same as *response costs*
Danger	Same as *threat*
Danger control	Same as *adaptive behavior*
Extrinsic maladaptive rewards	*Extrinsic* rewards for engaging in the maladaptive response of not protecting oneself, such as monetary compensation (Floyd et al. 2000; Rogers and Prentice-Dunn 1997)
Fear	A negatively valenced emotion representing a response that arises from recognizing danger. This response may include any combination of apprehension, fright, arousal, concern, worry, discomfort, or a general negative mood, and it manifests itself emotionally, cognitively, and physically (Leventhal 1970; McIntosh et al. 1997; Osman et al. 1994; Witte 1992; 1998; Witte et al. 1996)
Fear appeal	A purposefully generated message that is carefully designed and manipulated first to raise perceptions of threat severity and vulnerability and the subsequent fear, and then to invoke one's sense of self-efficacy and response efficacy, all of which are intended to overcome maladaptive rewards and response costs and subsequently change one's intentions toward an adaptive response (Floyd et al. 2000; Fry and Prentice-Dunn 2005, 2006; Milne et al. 2000; Rogers and Prentice-Dunn 1997)
Fear control	Same as *maladaptive behavior*
Intrinsic maladaptive rewards	*Intrinsic* rewards for engaging in the maladaptive response of not protecting oneself, such as maintaining pleasure or exacting revenge (Floyd et al. 2000; Rogers and Prentice-Dunn 1997)
Maladaptive behavior	Purposefully avoiding a danger-control response in response to a fear appeal and choosing a behavior that is not protective against the danger raised in the fear appeal (Floyd et al. 2000; Rogers and Prentice-Dunn 1997). Can be further conceptualized as intrinsic and extrinsic maladaptive rewards, but this is not required
Maladaptive coping response	Same as *maladaptive behavior*
Maladaptive rewards	The general rewards (intrinsic and extrinsic) of not protecting oneself, contrary to the fear appeal (Floyd et al. 2000; Rogers and Prentice-Dunn 1997)
Negative rewards	Same as *maladaptive rewards*
Perceived severity	Same as *threat severity*
Perceived susceptibility	Same as *threat vulnerability*
Perceived vulnerability	Same as *threat vulnerability*

Table C1. Key Terms and Concepts in Fear-Appeals Research (Continued)	
Term/Concept	**Definition (Citation)**
Protection motivation	One's intentions to protect oneself from the danger raised in the fear appeal
Protective behavior	Same as *adaptive behavior*
Response costs	"Any costs (e.g., monetary, personal, time, effort) associated with taking the adaptive coping response" (Floyd et al. 2000, p. 411)
Response efficacy	"The belief that the adaptive [coping] response will work, that taking the protective action will be effective in protecting the self or others" (Floyd et al. 2000, p. 411; Maddux and Rogers 1983)
Self-efficacy	"The perceived ability of the person to actually carry out the adaptive [coping] response" (Floyd et al. 2000, p. 411; Maddux and Rogers 1983)
Threat	The danger raised in the fear appeal that threatens one's safety
Threat appraisal	The process of considering the severity of and vulnerability to a threat against the maladaptive rewards associated with a maladaptive behavior, such as saving time or avoiding trouble by not following the response advocated for in the fear appeal (Floyd et al. 2000; Rogers and Prentice-Dunn 1997)
Threat severity	"How serious the individual believes that the threat would be" to him- or herself (Milne et al. 2000, p. 108)
Threat susceptibility	Same as *threat vulnerability*
Threat vulnerability	"How personally susceptible an individual feels to the communicated threat" (Milne et al. 2000, p. 108)

References

Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. 2000. "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology* (30:2), pp. 407-429.

Fry, R. B., and Prentice-Dunn, S. 2005. "The Effects of Coping Information and Value Affirmation on Responses to a Perceived Health Threat," *Health Communication* (17:2), pp. 133-147.

Fry, R. B., and Prentice-Dunn, S. 2006. "Effects of a Psychosocial Intervention on Breast Self-Examination Attitudes and Behaviors," *Health Education Research* (21:2), pp. 287-295.

Leventhal, H. 1970. "Findings and Theory in the Study of Fear Communications," in *Advances in Experimental Social Psychology,* L. Berkowitz (ed.), New York: Academic Press, pp. 119-186.

Maddux, J. E., and 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), pp. 469-479.

McIntosh, D. N., Zajonc, R. B., Vig, P. S., and Emerick, S. W. 1997. "Facial Movement, Breathing, Temperature, and Affect: Implications of the Vascular Theory of Emotional Efference," *Cognition & Emotion* (11:2), pp. 171-195.

Milne, S., Orbell, S., and Sheeran, P. 2002. "Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and Implementation Intentions," *British Journal of Health Psychology* (7:May), pp. 163-184.

Osman, A., Barrious, F. X., Osman, J. R., Schneekloth, R., and Troutman, J. A. 1994. "The Pain Anxiety Symptoms Scale: Psychometric Properties in a Community Sample," *Journal of Behavioral Medicine* (17:5), pp. 511-522.

Rogers, R. W., and Prentice-Dunn, S. 1997. "Protection Motivation Theory," in *Handbook of Health Behavior Research I: Personal and Social Determinants,* D. S. Gochman (ed.), New York: Plenum Press, pp. 113-132.

Witte, K. 1992. "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," *Communication Monographs* (59:4), pp. 329-349.

Witte, K. 1998. "Fear as Motivator, Fear as Inhibitor: Using the Extended Parallel Processing Model to Explain Fear Appeal Successes and Failures," in *Handbook of Communication and Emotion: Research, Theory, Application, and Contexts,* P. A. Anderson, and L. K. Guerrero (eds.), San Diego, CA: Academic Press, pp. 423-450.

Witte, K., Cameron, A., McKeon, J. K., and Berkowitz, J. M. 1996. "Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale," *Journal of Health Communication* (1:4), pp. 317-342.