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.