Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-15-2012

Examining the Coping Appraisal Process in End User Security

Kent Marett
Mississippi State University, kent.marett@msstate.edu

Nirmalee Ratnamalala
Mississippi State University

Examining the Coping Appraisal Process in End User Security

Kent Marett[1]
College of Business, Mississippi State University,
Mississippi State, MS, USA

Nirmalee Ratnamalala
College of Business, Mississippi State University,
Mississippi State, MS, USA

ABSTRACT

Protection Motivation Theory, which models the appraisal processes individuals make in regard to potential threats and safeguards, has informed a number of previous empirical studies on information security. However, none have accounted for the possibility of multiple countermeasures. In this study, we investigated this possibility by analyzing the responses of computer users who could potentially suffer malware infections. Initial results suggest that high levels of self-efficacy and low levels of response costs motivate the intentions to adopt one countermeasure over another.

Keywords: Protection Motivation Theory, Coping Appraisal, Response Costs, Self-Efficacy, Malware

INTRODUCTION

Individuals and organizations deal with an enormous amount of information on a daily basis. Much of this information needs to be secured from potential intruders. As a measure of ensuring information security, it is imperative for individuals and organizations to consider available countermeasures to help protect their secure information from unauthorized access. Previous studies in the area of information security have adopted the Protection Motivation

[1] Corresponding author. kent.marett@msstate.edu. +1 662 325 7001

Theory (PMT) as a means predicting an individual's behavioral intention to protect oneself against malware, viruses, hacking, insider threat, social engineering, and password compromise, among other threats to information (Herath and Rao 2009; Johnston and Warkentin 2010; Marett et al. 2011). Generally speaking, PMT explains how the perceptual variables of threat severity, threat vulnerability, self-efficacy, response efficacy and response cost influence an individual's intention to adopt a certain response or countermeasure.

PMT models two sequential cognitive processes, a threat appraisal and a coping appraisal, as having an influence on behavioral intent. In the first process, the threat appraisal, the perceived severity and vulnerability associated with the threat are hypothesized to have a positive relationship with behavioral intention, with the perceived rewards associated with continuing one's risky behavior negating some of that relationship. The current study focuses on the second process, the coping appraisal, which focuses on the methods by which the individual may counter the threat. PMT theorizes that individuals appraise the response efficacy of a countermeasure and their own self-efficacy in successfully implementing it, both of which are expected to positively influence behavioral intent. Coping appraisals also include the influence of the perceived response costs associated with the countermeasure, which are expected to negatively influence behavioral intent.

For each potential threat to one's security and privacy, the threat appraisal process is likely conducted once at that time. However, there may be multiple possible countermeasures to the threat, which suggests that individuals could undertake the coping appraisal process multiple times before deciding on a course of action. To our knowledge, this has seldom been acknowledged in previous PMT research, especially those in the field of information security. Thus, the research questions of this study are (a) do individuals differentiate between multiple

countermeasures when engaging in protection motivation, and (b) how does this differentiation affect behavioral intentions to protect oneself?

THEORY REVIEW

PMT was developed by Rogers (1975) to help explain the cognitive processes people use when appraising risks to their health (Floyd et al. 2000). As described earlier, PMT consists of two main components, the threat appraisal and coping appraisal. The threat appraisal process is initiated first since an individual needs to recognize the threat prior to assessing the coping behaviors. Perceived threat severity is the belief of the significance or the magnitude of the threat whereas perceived threat vulnerability is an individual's belief of the probability of experiencing a certain threat (Ifinedo 2012). Rewards include the extrinsic and intrinsic benefits gained by an individual for not following the recommended response. The threat appraisal process is triggered by the realization of an external influence associated with the individual's behavior that is potentially a source of negative consequences.

Should the individual determine the threat can cause a degree of harm that the individual seeks means of protection against it, the coping appraisal process is initiated. Self-efficacy is an individual's belief that s/he will be able to carry out the recommended response by themselves whereas response efficacy is the belief that a particular response is adequate in protecting oneself (Floyd et al. 2000). Response costs are any related costs in carrying out the recommended response. Taken together, protection motivation involves any threat for which there is an effective recommended response that can be carried out by the individual. For example, for a threat of lung cancer due to smoking, a recommended response is to quit smoking, and to guard

against the threat of injury from a car crash, a recommended response would be to wear a seat belt. In terms of information security, the threat of computer virus infection has a recommended response to install anti-virus software, and for a threat of unexpected data loss, a recommended response would be to frequently back up data.

Much of the extant literature on protection motivation has paired a specific threat with one recommended response, but conceivably, there could be multiple effective responses. Studies that have acknowledged this possibility are few and far between. In his meta-analysis of PMT studies in the health communication field, Floyd et al. (2000) indicates that a limited number of studies have offered a variety of different recommended responses for a given threat, but when they have, the coping appraisal variables have been observed to influence the choice of response. For instance, participants considering the threat of skin cancer indicated that completely staying out of the sun has a greater response cost than using sunscreen, and was thus the less popular option (Jones and Leary 1994). Similarly, people in the aftermath of Hurricane Lili were found to differ in their action plans for future storms based on the relative response costs of preparation and implementation (Kang et al. 2007). Research on the consequences of binge drinking suggests that, when identifying multiple strategies to avoid negative consequences, individuals choose the strategy that has personally been most effective for managing risks in the past (i.e., response efficacy) (Wolburg 2001). Whether these coping appraisal variables influence which among multiple countermeasures chosen by individuals considering a threat to information security remains to be seen.

Self-Efficacy

Within the context of protection motivation, self-efficacy is the belief of an individual on his or her own ability to carry out a recommended response and successfully avert a threat

(Milne et al. 2000). A person's self-efficacy has been speculated as being a source of motivation to more frequently and more persistently engage in implementing information security coping responses (Rhee et al. 2009). A number of PMT studies focusing on intentions to adopt better security behaviors and countermeasures have found a strong positive relationship between self-efficacy and behavioral intentions (Gurung et al. 2009; Ifinedo 2012; Johnston et al. 2010; Lee 2011). However, we expect that, when comparing possible responses, an individual will be more likely to adopt the recommended response he or she feels more confident in his or her ability to implement it. Therefore:

H1: Given multiple responses for protecting against a threat to information security, individuals will intend to adopt the response or responses with higher perceived self-efficacy.

Response Efficacy

Response efficacy is an individual's assessment of the chance a recommended response will be effective in averting the specific threat or danger (Milne et al. 2000). When an individual feels that a specific response will be effective in reducing the threat, the likelihood of the individual to adopt the recommended response will increase. The choice of a response that appears to have a greater chance for success could be a question of resource allocation (Herath et al. 2009) in that individuals assessing a significant threat will tend to choose a "sure thing" over an untested alternative if there is no slack time or resources to absorb a failure. Perceived response efficacy has been consistently found to be a significant positive influence on behavioral intentions (Johnston et al. 2010). Therefore we hypothesize that:

H2: Given multiple responses for protecting against a threat to information security, individuals will intend to adopt the response or responses with higher perceived response efficacy.

Response Costs

Response costs refer to any cost such as time, money, effort incurred due to carrying out a recommended response (Floyd 2000; Milne et al. 2000). Should an individual perceive the cost of a response to be higher than the benefits it provides or than the cost caused by the threat being realized, the individual is less likely to adopt that response. In terms of information security behaviors, the role of response costs toward implementing less risky security controls has been mixed. In some studies, individuals were influenced to adopt a behavior or countermeasure based on the costs they expected to incur (Hu and Dinev 2005; Workman et al. 2008), while other studies did not find response cost to significantly influence behavioral intentions (Gurung et al. 2009; Lee and Kozar 2005). In some cases, the measure for response costs could have been inadvertently assessed the perceived ease of use (i.e. "I am able to implement this control without much trouble"), which would likely confound with the measure for self-efficacy (Chenoweth et al. 2009). In other studies, assessing response costs has been more likely to produce maladaptive behaviors (avoidance or hopelessness) than the adoption of a secure behavior (Marett et al. 2011). In the present study, given a set of recommended responses, response cost will negatively influence the end user in adopting a recommended response. Therefore:

H3: Given multiple responses for protecting against a threat to information security, individuals will intend to adopt the response or responses with lower perceived response costs.

METHOD

An online survey was administered to the undergraduate and graduate students in the college of business at a southern university and their acquaintances via "snowball sampling" where the study participants were requested to recruit additional participants for the study.

Participants appraised the threat of malware, which was defined for them as "malicious software programmed to access a computer system without the authorization of its owner" and includes computer viruses, spyware, and Trojan horses (Malimage and Warkentin 2011). In addition to being a concept most Internet users are aware of, malware has been observed as a serious threat in previous PMT research, with individuals eagerly seeking out methods by which to reduce its likelihood (Lee and Larsen 2009). Three countermeasures were provided as ways to cope with the threat: users should keep virus detection software updated, users should enable firewalls on their computer, and users should avoid visiting suspicious or untrusted websites. These countermeasures have been used in PMT studies and have been recommended as safeguards by major software developers and universities[2]. In terms of the response costs placed on the average Internet user, keeping virus detection definitions current was expected to be the most demanding response, followed by enabling firewalls and then by avoiding suspicious websites (Stafford and Poston 2010). The survey effort produced 146 usable responses. The average age of respondents was 21.8 years and the sample was 50.3 percent female. There was no attempt made to identify the setting (work, home, etc.) in which the respondent's computer resides nor the operating system and its inherent vulnerabilities installed on the computer.

All items in the instrument (see Table 1) were adopted from previously developed scales and passed an expert panel review. Respondents were requested to rate the level of severity and vulnerability for the threat of malware infection. The respondents were then presented with the three recommended responses (in random order) accompanied by items measuring the individual's perceived self-efficacy, response efficacy and response costs for each. Survey

[2] The three recommended responses for preventing malware infection are listed on the help reference websites for both Apple and Microsoft, as well as on the helpdesk websites for Cornell University, Mississippi State University, and Texas A&M University.

respondents did consider the threat of malware to be severe (M=3.72 on 5-point scale) and considered themselves above average in vulnerability (M=3.04).

Table 1. Items for PMT Measures.

Measure	Item
Threat Severity (Johnston et al. 2010)	1) If my computer were infected by malware, it would be significant. 2) If my computer were infected by malware, it would be severe. 3) If my computer were infected by malware, it would be serious.
Threat Vulnerability (Johnston et al. 2010)	1) It is possible that my computer will become infected with malware. 2) It is likely that my computer will become infected with malware. 3) My computer is at risk for becoming infected with malware.
Self Efficacy (Gurung et al. 2009)	1) I have the skills to install a personal firewall. 2) I am able to install a personal firewall. 3) I am capable of installing a personal firewall.
Response Efficacy (Lee 2011)	1) A personal firewall is effective for protection against malware. 2) Malware can be prevented by using a personal firewall. 3) A personal firewall works for protection against malware.
Response Costs (Workman et al. 2008)	1) It is inconvenient to install a personal firewall. 2) It is time consuming to install a personal firewall. 3) It is troublesome to install a personal firewall.
Behavioral Intent to Adopt Response (Johnston et al. 2010)	1) I intend to install a personal firewall in the near future. 2) I plan to install a personal firewall in the near future. 3) I predict I will to install a personal firewall in the near future.

Analysis

Before conducting the main data analysis, we performed a confirmatory factor analysis for the items and measures derived from PMT, and found that all of the modeled items loaded most strongly on their associated measure. We then assessed the reliability and discriminant validity of the measures. Reliabilities were assessed using Cronbach's Alpha, and each of the

measures were found to surpass the recommended value of 0.7. Finally, we determined that the measures demonstrated discriminant validity by comparing the square root of the average variance extracted with the inter-construct correlations for each. In the cases of the behavioral intent, response and self efficacy, and response cost measures, the reliability and validity checks were performed separately for each of the three responses.

Table 2. Results of Paired Sample T-tests. Means (Standard Deviations).

	Anti-Virus Software (AV)	Personal Firewall (PW)	Avoid Untrusted Websites (UW)	Significant Differences
Self Efficacy	3.89 (0.9)	3.87 (0.8)	4.14 (0.7)	AV – UW ** PW – UW **
Response Efficacy	3.98 (0.6)	3.94 (0.6)	3.97 (0.8)	all n.s.
Response Costs	2.93 (1.0)	2.69 (0.8)	2.56 (0.8)	AV – UW ** AV – UW **
Behavioral Intent to Adopt	3.64 (0.9)	3.82 (0.8)	4.13 (0.7)	all **

NOTE: ** p<.01, * p<.05, n.s. = not significant

We first tested the hypotheses using paired sample comparisons of the coping appraisal variables across the three responses, the results of which can be found in Table 2. The goal of this analysis was to confirm that the three recommended responses could be differentiated by computer users. Respondents perceived the option to avoid untrusted websites differently in terms of self-efficacy, they reported significant differences in response costs for updating anti-virus software, and BI to adopt was significant between all three responses, which suggests that the responses could be appraised differently. The most likely response to be adopted was avoiding untrusted websites, and it was rated the highest in perceived self-efficacy and lowest in

response costs, supporting Hypotheses 1 and 3. There was no significant difference in response efficacy between the three responses, effectively voiding Hypothesis 2.

We next determined the influence of the two appraisal processes on the behavioral intentions to adopt each of the three responses. This was performed through hierarchical linear regression analyses, which has been used in previous PMT studies to account for the time order of the appraisal processes (Grothmann and Reusswig 2006; Marett et al. 2011). The first regression model included the threat appraisal variables, and the second model added the coping appraisal variables. The results of these regression analyses can be found in Table 3.

Table 3. Results of Hierarchical Regression. Standardized Betas Displayed.

Dependent Variable: BI to Adopt Response →	EV	Anti-Virus Software		Personal Firewall		Avoid Untrusted Websites	
Threat Appraisal							
Threat Severity	+	.11	-.01	.07	-.03	.39**	.12
Threat Vulnerability	+	.21**	.29**	.06	.18**	-.01	.02
Coping Appraisal							
Response Efficacy	+		.24**		.53**		.38**
Self-Efficacy	+		.31**		.31**		.37**
Response Costs	-		-.14		-.13*		-.09
R^2		.31		.63		.58	
Adjusted R^2		.29		.61		.56	
ΔR^2 from Threat to Coping		.24**		.59**		.43**	
F		12.46**		46.83**		38.13**	

EV = Expected Valence. ** p< .01, * p< .05

DISCUSSION

The main focus of this study was to examine the coping appraisal process undertaken by computer users who are advised to choose among multiple countermeasures to better protect oneself from a threat to their security. Although the possibility of multiple responses seems to exist with most security threats, it has yet to be accounted for in the IS security literature. Among

our findings, high levels of self-efficacy and low levels of response costs were associated with the countermeasure most intended to be adopted. Further, the increase in variance explained by the coping appraisal alone suggests that, when multiple countermeasures are under consideration, the coping variables (particularly, self-efficacy and response efficacy) were more influential toward the decision to adopt than those for the threat appraisal. In all, our results suggest that, when faced with multiple protective responses, the coping appraisal may take a more prominent role in decision-making than previous research has indicated, and coping variables like self-efficacy and response costs may influence a user's choice of response should each be perceived as being equally effective.

Our results also suggest that a user's perception of response costs should be better acknowledged in future information security studies informed by PMT. Increased security typically comes at the sacrifice of convenience, and any perceived hindrance can be reason enough for users to fail to comply with existing security policies (Herath et al. 2009), much less for adopting new countermeasures. However, future research is needed to determine to what extent a protective action is taken and whether the perceived costs involved take a different role over the long term (Grothmann et al. 2006). Here, the act of avoiding untrusted websites was reportedly the least costly response, but the choice to browse risky websites could be a more situational decision than the other two responses in this study and, thus, cause an individual to re-evaluate the protective behavior.

The results should be interpreted with the following limitations in mind. First, we selected one specific threat to information security and three specific responses to examine. We hesitate to presume that a different threat or other responses would produce the same appraisal. We also did not provide a fear appeal to serve as a catalyst for the threat appraisal process, so

whatever perceived severity of or vulnerability to malware was reported by our respondents was likely a product of their own previous experience. Also, the survey respondents were mostly college students, but the snowball sampling method attempted to extend beyond that group of individuals. Nonetheless, all of the respondents reported using a computer over five hours a week. Thus, the threat of malware was salient to the sample.

A key component to rational decision-making is the process of identifying all reasonable alternatives and appraising each for their suitability. This study is a first step in taking that concept and applying it to the context of protection motivation. Information security practitioners must acknowledge that users may instead satisfice and choose the easiest, least costly solution. In these cases, we must attempt to make effective responses readily available.

REFERENCES

Chenoweth, T., Minch, R., and Gattiker, T. "Application of Protection Motivation Theory to Adoption of Protective Technologies," Paper presented at the 42nd Hawaii International Conference on System Sciences, Big Island, HI, 2009.

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

Grothmann, T., and Reusswig, F. "People at Risk of Flooding: Why Some Residents Take Precautionary Action While Others Do Not," *Natural Hazards* (38) 2006, pp. 101-120.

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

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

Hu, Q., and Dinev, T. "Is Spyware an Internet Nuisance or Public Menace?" *Communications of the ACM* (48) 2005, pp. 61-66.

Ifinedo, P. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1) 2012, pp. 83-95.

Johnston, A., and Warkentin, M. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3) 2010, pp. 549-566.

Jones, J., and Leary, M. "Effects of Appearance-Based Admonitions against Sun Exposure on Tanning Intentions in Young Adults," *Health Psychology* (13) 1994, pp. 86-90.

Kang, J.E., Lindell, M., and Prater, C. "Hurricane Evacuation Expectations and Actual Behavior in Hurricane Lili," *Journal of Applied Social Psychology* (37:4) 2007, pp. 887-903.

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

Lee, Y., and Kozar, K. "Investigating Factors Affecting the Adoption of Anti-Spyware Systems," *Communications of the ACM* (48) 2005, pp. 72-77.

Lee, Y., and Larsen, K. "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems* (18:2) 2009, pp. 177-187.

Malimage, K., and Warkentin, M. "Influence of Perceived Value of Data on Anti-Virus Software Usage: An Empirical Study of Protection Motivation," Paper presented at the Dewald Roode Workshop on Information Systems Security Research, Blacksburg, VA, 2011.

Marett, K., McNab, A., and Harris, R.B. "Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory," *AIS Transactions on Human-Computer Interaction* (3:3) 2011, pp. 170-188.

Rhee, H.-S., Kim, C., and Ryu, Y. "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior," *Computers & Security* (28:8) 2009, pp. 816-826.

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

Stafford, T., and Poston, R. "Online Security Threats and Computer User Intentions," *Computer* (43:1) 2010, pp. 58-64.

Wolburg, J. "The 'Risky Business' of Binge Drinking among College Students: Using Risk Models for PSAs and Anti-Drinking Campaigns," *Journal of Advertising* (30:4) 2001, pp. 23-39.

Workman, M., Bommer, W.H., and Straub, D. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24:6) 2008, pp. 2799-2816.