Putting the 'Motivation' in Protection Motivation Theory: An Examination of Persuasive Communication via Extrinsic and Intrinsic Means

Research-in-Progress

Philip Menard
Mississippi State University
philip.menard@msstate.edu

Abstract

Protection Motivation Theory (PMT) has been widely adapted to the context of behavioral information security research, but results have not been as consistent as studies in PMT's native disciplines. One construct that may provide greater explanatory power in InfoSec contexts is motivation. One of the key elements of effective applications of PMT is the use of fear appeals, which focus on the danger of an outside threat and may be classified as a more control-oriented (i.e. extrinsic) form of communication. Motivation may provide an interesting counterpoint to prior PMT research by incorporating self-determined (i.e. intrinsic) forms of persuasive communication in motivating the end user to perform secure behaviors related to information protection. A research model and experimental design are proposed to capture the differences in end user perceptions due to applications of intrinsic or extrinsic forms of communication. Potential implications for research and practice are discussed.

Keywords: protection motivation theory; self-determination theory; information security; persuasive communication

Introduction

Information security continues to be a significant concern for both organizations and home computer users. Large firms, including Apple, Twitter, and Facebook, have recently been victims of data breaches, highlighting the significance of information security at the organizational level (Gross 2013). However, hackers have not limited themselves to targeting corporations, with 61% of computer users having experienced some type of malware attack (Richardson 2011). A common delivery mechanism for these attacks is via the propagation of malicious software infecting end users' machines. Hackers may target the infected machine for valuable data or utilize a series compromised computers to create botnets intended for attacking other targets. The level of global connectivity users experience via the Internet creates an environment ripe for hackers to distribute and replicate malware across end users' machines. As telecommuting continues to grow in popularity among organizations, an individual may use his or her personal computer at home to perform business functions, demonstrating the need for end users to practice secure computing behaviors at home as well as at the workplace. Failure to implement the right security procedures may place both the user's computer and the company at risk. This may manifest through a hacker using a compromised personal computer as a conduit to infiltrating organizational information assets. The loss of private data may result in identity theft or heightened privacy concerns of individuals.

While many computer-related security procedures have become automated to ensure proper implementation and utilization, certain security measures are still dependent on the actions of end users. For this reason, humans are typically considered the weakest link in maintenance of secure information environments (Sasse et al. 2001). Researchers examining behavioral information security have drawn upon theories from a variety of outside behavioral disciplines to determine the underlying reasons why end users may or may not perform secure behaviors. Protection Motivation Theory (PMT) has subsequently become one of the most commonly adapted theories in behavioral information security studies (Herath and Rao 2009; Johnston and Warkentin 2010; Pahnila et al. 2007; Workman et al. 2008).

Although PMT has been commonly used to explain the adoption of secure behaviors in information security research, this theory assumes that individuals make decisions regarding secure behaviors based on cognitive appraisals. However, not all behaviors can be explained by cognitive reasoning. Rather, they may be due to other factors, such as affect or habit (Vance et al. 2012). An individual's propensity to be either intrinsically or extrinsically motivated may also play a role in forming intentions to perform secure behaviors.

An important delivery tool for communicating the seriousness of the threat and the appropriate response is the fear appeal. Despite the success of fear appeal campaigns related to vehicular safety or smoking cessation (Floyd et al. 2000), the fear appeal may be categorized as an extrinsic form of motivation due to its focus on external entities that may or may not be related to the individual (Ryan 1982). Significant differences have been shown between groups receiving control-oriented and self-determined communications (Ryan et al. 1983), demonstrating that different outcomes may be experienced whether the individual is intrinsically or extrinsically motivated through the information provided.

Additionally, intrinsically motivated individuals are more likely to engage in rational decision-making processes (Vallerand 1997). While autonomous individuals may also be extrinsically motivated, they are able to internalize certain external forces and focus on utilizing these forces to achieve autonomous goals (Deci and Ryan 1980). Rather than internalizing the threat and coping appraisal components of PMT, an extrinsically motivated individual may act based solely on external forces dictating his or her behavior without engaging in a cognitive understanding of why performing such a behavior is important. Using PMT and prior research in motivation as a foundation, this study aims to answer the following research questions:

1. Do intrinsically motivated individuals cognitively assess the threat and coping components of PMT differently than extrinsically motivated individuals?
2. Does persuasive communication focused on self-determined motivation foster greater intentions to perform secure behaviors among end users than traditional fear appeals?
3. Does perception of motivation have an effect on behavioral intention to perform secure behaviors?

The remainder of this paper is structured as follows. First the relevant literature associated with PMT will be reviewed, upon which our research model is based. This is followed by an examination of the salient theoretical foundation of self-determination theory and linkages which may exist between motivation and prior studies in information security. We then propose our conceptual model, along with supporting hypotheses used to test the model. The next section discusses the research method and data analysis to be performed. The paper closes with discussion of the proposed contributions to research and practice.

Literature Review and Hypothesis Development

Protection Motivation Theory

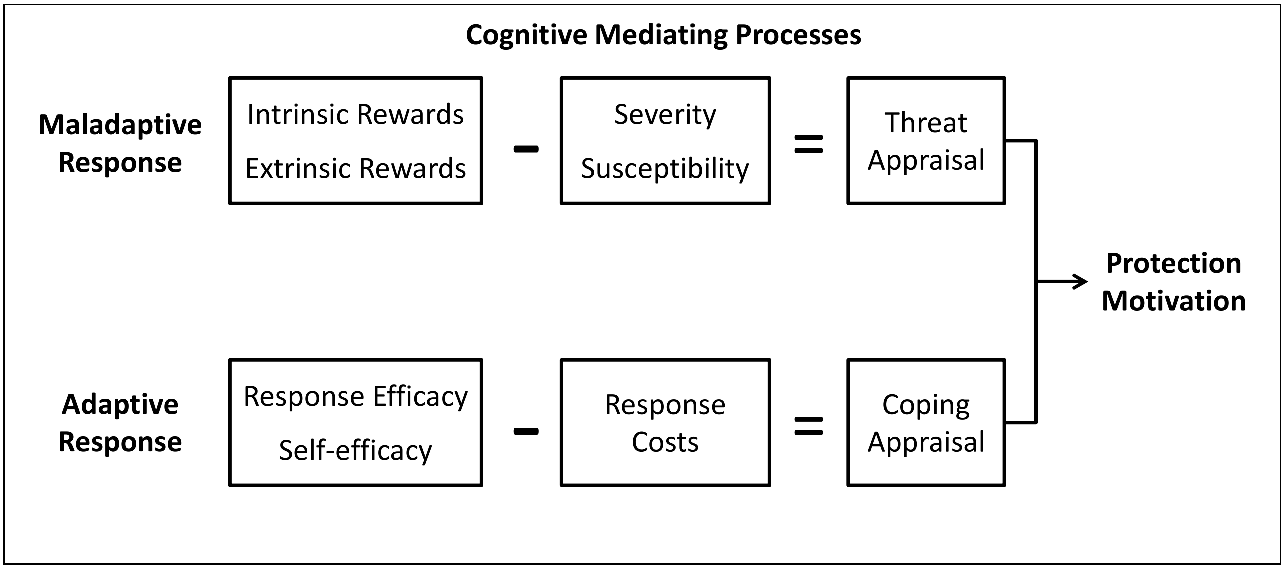

Figure 1. Protection Motivation Theory (Floyd et al. 2000)

Protection Motivation Theory, or PMT, was originally introduced by Rogers (1975), and later modified and expanded (1983), in the context of health safety and awareness. PMT posits that when someone is presented with a threat, he or she goes through a cognitive process of threat appraisal and coping appraisal. After assessing the threat and its associated coping mechanisms, one decides to perform either adaptive or maladaptive behaviors. Adaptive behaviors are recommended responses that are intended to protect someone against the threat, whereas maladaptive responses can be a range of activities in which the respondent avoids performing the recommended responses.

In the context of IS security research, PMT is highly applicable due to the tangible threat-response pairs evident in IS security. Consequently it is one of the most widely adapted theories in our field. Perhaps most relevant to the present study, Johnston and Warkentin (2010) propose a Fear Appeal Model in information security where the imminent threat of harmful spyware is communicated to the users, with users also receiving information about an easy-to-use anti-spyware tool to effectively protect their computers, similar to the threat-response pair described earlier. Their research has informed our study of the use of motivational communications to encourage end users to take protective measures concerning information assets. However, this study aims to provide a contrast to messages containing fear appeals by offering an appeal to the end user which emphasizes an intrinsic motivation to perform secure behaviors. PMT is used as the primary foundation for the conceptual model in this study as well.

Self-Determination Theory

The results of information security related PMT studies have not been as consistent as those developed in PMT's native discipline of health care (Crossler et al. 2013). This could be due to applications in health care where the threat and coping appraisal are related directly to protection of the individual, whereas in information security the threat and coping mechanisms are related to protection of information related to the individual or data with which the individual may interact. Because of the degree of separation between the individual and the information, other constructs may have the opportunity to influence an individual's perception of threat-response pairs.

Motivation may contribute to the influence of a user's intention to perform secure behaviors. Motivation can be broadly classified as intrinsic or extrinsic (Deci 1972; Ryan and Deci 2000a). An individual can also experience a deficiency of motivation, referred to as amotivation (Ryan and Deci 2000a). Intrinsic motivation is defined as "performing an activity for itself, and the pleasure and satisfaction derived from participation" (Vallerand 1997). Extrinsic motivation is defined as "engaging in an activity as a means to an end and not for its own sake" (Vallerand 1997).

After a stream of research comparing intrinsic and extrinsic motivation with mixed results, Deci and Ryan (1980) developed Self-Determination Theory (SDT), which classifies distinct forms of extrinsic motivation, each possessing different levels of self-determined, or autonomous, origins (see Figure 2). On the opposite end of the self-determined continuum are control-oriented forms of extrinsic motivation, which are characterized by the degree to which the motivation is derived outside of the individual. There are four types of extrinsic motivation: external regulation, introjected regulation, identified regulation, and integrated regulation. External regulation refers to regulating behavior through external means, such as rewards or constraints. Introjected regulation occurs when an individual internalizes the reasons for his or her actions, meaning the motivation is internal but not self-determined. Identified regulation occurs when behavior is highly valued and judged as important upon identification. Integrated regulation refers to choices that are made as a function of their coherence with other aspects of the self. These various types of extrinsic motivation also vary according to the level of self-determination present.

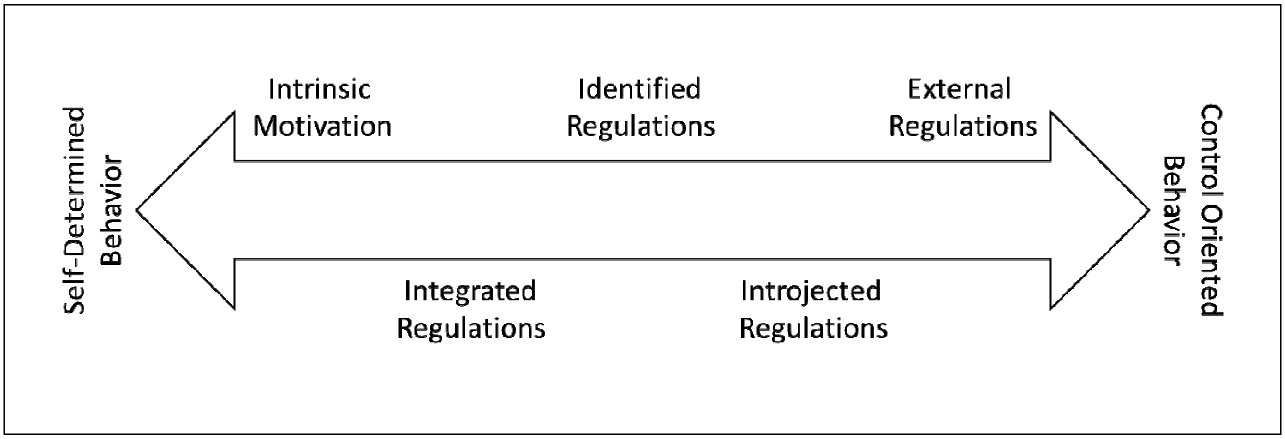

Figure 2: Types of Motivation along the Self-Determined Continuum (Deci & Ryan 1980)

High levels of autonomy, relatedness, and competence have been shown to increase intrinsic motivation and decrease amotivation and control-oriented forms of extrinsic motivation, while low levels of autonomy, competence, and relatedness have the reverse effect (Deci and Ryan 1980; Ryan et al. 1983; Vallerand 2000). Autonomy refers to one's perception of the degree to which he or she may engage in activities of his or her own desire. Perceptions of competence relate to the degree to which an individual feels he or she can interact effectively with his or her surroundings in order to produce desired outcomes or prevent undesired consequences. Relatedness is one's perception of the degree to which he or she feels connected with others (Vallerand et al. 1997). Despite the influence of these variables, researchers examining effective communications of relevant security threats have focused on inducing secure behavior through the use of fear appeals, which are centered on what appear to be control-oriented motivational techniques (Johnston and Warkentin 2010; Pahnila et al. 2007; Workman et al. 2008). By focusing on the threat, individuals may be engaged in a behavior that is not self-determined, due to the nature of the threat deriving from an external party. Embedding varieties of intrinsic motivation or more self-determined forms of extrinsic motivation within information security appeals may influence an end user's performance of secure behaviors through the application of intrinsic rather than extrinsic motivation.

Using Deci and Ryan's foundational work on motivation (Deci and Ryan 1980; Deci 1972; Ryan 1982), Vallerand (1997) developed a hierarchical model of motivation, separating one's motivation into global, contextual, and situational levels. Global level motivation is one's general motivational orientation to interact with the environment. The next lower level, contextual level motivation, is one's usual motivational orientation toward a specific context, such as education, work, leisure, or interpersonal relationships. Finally, situational level motivation is the motivation individuals experience when they are currently engaging in an activity within a specific context. Vallerand's hierarchical model demonstrates that although motivation may be classified as a stable trait, such as one's global-level motivation, individuals may be intrinsically or extrinsically motivated depending on the specific situation, regardless of a general inclination toward self-determined or control-oriented motivation.

Research Model and Hypothesis Development

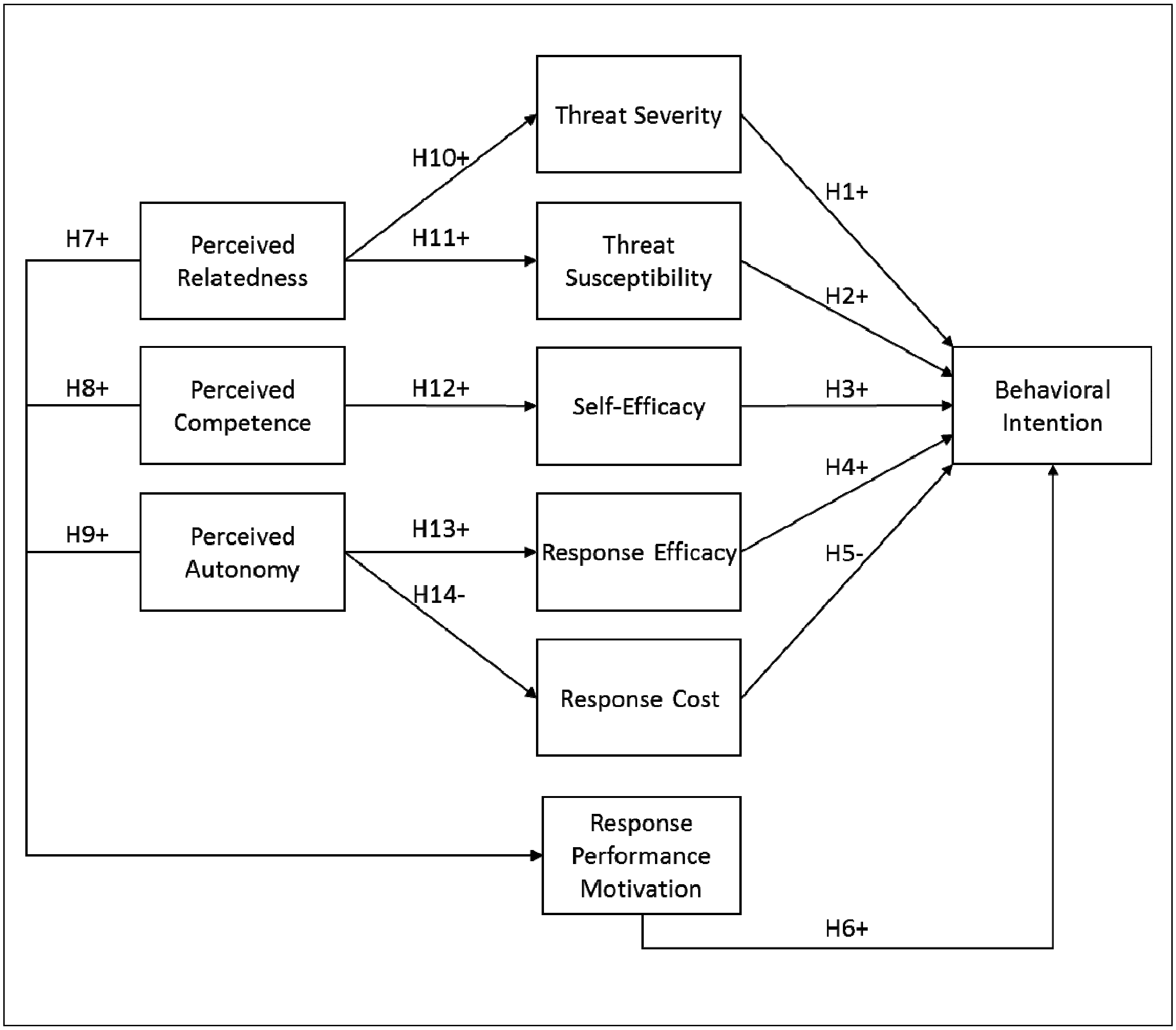

Figure 3: Research Model

A critical aspect of protection motivation theory is the presumption that an individual initiates a cognitive process of evaluating a particular threat, both on its severity and the likelihood of such a threat affecting that person (Floyd et al. 2000; Rogers 1975). For example, as an end user's perception of the amount of danger associated with spyware increases, the individual will form intentions to perform the recommended response for mitigating the threat. Similarly, if an individual perceives that the probability of becoming infected with spyware as extremely likely, he or she will form intentions to perform the recommended response. These relationships have been posited throughout the existence of PMT, and empirical evidence of these hypotheses has been demonstrated extensively in prior research (Floyd et al. 2000; Herath and Rao 2009; Pahnila et al. 2007). Thus, the following hypotheses are presented:

> *H1: End user perceptions of threat severity will positively influence behavioral intention to perform secure behaviors.*

> *H2: End user perceptions of threat susceptibility will positively influence behavioral intention to perform secure behaviors.*

Another important element of PMT is the relationship between an individual's coping mechanism and intention to perform secure behaviors. The coping appraisal, consisting of response efficacy, self-efficacy, and response cost, has also been extensively researched in studies adapting PMT. After cognitively processing attributes of the present threat, an individual conducts another cognitive assessment on ways in which the threat may be mitigated. As an individual's perception of the effectiveness of a particular response increases, his intention to use that response increases. If the individual is confident in his or her ability to perform the response, intentions also increase. As the cost of performing the response, which may be comprised of various factors such as money, time, convenience, or effort, increases, the individual's intention to execute the recommended response wanes. The relationships between coping appraisal variables and intention, like those associated with threat appraisal, have also been extensively examined in studies adapting PMT (Floyd et al. 2000; Johnston and Warkentin 2010; Workman et al. 2008). Likewise, we present the following hypotheses:

> *H3: End user perceptions of self-efficacy will positively influence behavioral intention to perform secure behaviors.*
>
> *H4: End user perceptions of response efficacy will positively influence behavioral intention to perform secure behaviors.*
>
> *H5: End user perceptions of response cost will negatively influence behavioral intention to perform secure behaviors.*

According to Vallerand's (1997) hierarchical model of motivation, one of the outcome variables of motivation is behavior. However, many studies in social psychology have examined the relationship between intentions and behavior, finding that the formation of intentions precedes the performance of the actual behavior (Ajzen and Fishbein 1980). The proposition of this relationship was first conceptualized by Fishbein and Ajzen's (1975) Theory of Reasoned Action (TRA). In their foundational study, Fishbein and Ajzen hypothesize that an individual's behavior is determined by a cognitive process in which intentions to perform the behavior are first conceived prior to actual performance of the behavior occurring. Adaptations of intention to perform a behavior have been widely used in information systems research (Davis et al. 1989; Venkatesh and Davis 2000; Venkatesh et al. 2003, 2012), as well as specifically in information security research (Bulgurcu et al. 2010; D'Arcy et al. 2009; Herath and Rao 2009; Johnston and Warkentin 2010). An individual who is intrinsically motivated to perform a secure behavior should consequently form intentions to execute that response. Thus, we hypothesize the following:

> *H6: End user motivation toward performing the recommended response will positively influence behavioral intention to perform secure behaviors.*

An individual's degree of self-determined motivation may be affected by his or her perceptions of competence, autonomy, and relatedness (Deci and Ryan 1980). If an individual feels that performance of the recommended response offers a sense of connection to the information being protected, his or her motivation will be more intrinsic. An individual perceiving high levels of competence related to performing a recommended response will be intrinsically motivated to perform the behavior. As an individual perceives a higher degree of autonomy related to the types of recommended responses available for mitigating the threat, his or her motivation will become more self-determined. Thus, the following hypotheses are offered:

> *H7: End user perceptions of relatedness will positively influence motivation toward performing the recommended response.*
>
> *H8: End user perceptions of competence will positively influence motivation toward performing the recommended response.*
>
> *H9: End user perceptions of autonomy will positively influence motivation toward performing the recommended response.*

Typically in motivational research, relatedness refers to the degree of connectedness an individual feels toward others when interacting in a specific context, such as school or work (Ryan and Deci 2000b;

Vallerand 1997, 2000). The root of an individual's need for relatedness is the emotional connection one may feel to a particular target, and the target may even be an inanimate object (Baumeister and Leary 1995; Thomson 2006). In this study, an individual's relatedness refers to his or her degree of connectedness with the information being threatened or in need of protection. If an end user experiences a deep connection with the data being protected, he or she may perceive the level of severity associated with the threat to be elevated. Similarly, he or she may also feel more susceptible to the threat if a connection with the data being protected exists. Accordingly, the following hypotheses are offered:

> *H10: End user perceptions of relatedness will positively influence perceptions of threat severity.*
>
> *H11: End user perceptions of relatedness will positively influence perceptions of threat susceptibility.*

In motivational research, one's competence refers to the level of confidence one perceives in a particular range of activities in which he or she is engaged (Deci and Ryan 1980). This concept is very similar to self-efficacy, which refers to an individual's belief in his or her ability to perform the specific task given as a recommended response to a threat (Floyd et al. 2000; Rogers 1983). The generality of competence and the specificity of self-efficacy designates that they are theoretically distinct constructs, but their conceptual similarity indicates that a relationship may exist between these two constructs. If an end user perceives a high degree of confidence related to performing activities related to securing information, he or she should experience an increase in self-efficacy to perform the particular recommended response communicated in the appeal. Thus, the following relationships are hypothesized:

> *H12: End user perceptions of competence will positively influence perceptions of self-efficacy.*

Autonomy refers to the self-regulation of one's behavior and the degree of governance one experiences toward the initiation and direction of his or her actions (Ryan 1991). Autonomy has been shown to have a powerful influence on individuals' perceptions of intrinsic motivation (Ryan and Deci 2000b; Vallerand 1997, 2000). In various motivational studies, autonomy is commonly operationalized as the presence of choice available to respondents along with allowing the respondents the freedom to select from those choices (Deci and Ryan 1987; Gagne and Deci 2005; Miserandino 1996; Reis et al. 2000). Studies in marketing have shown that when presented with choices, consumers' perceptions of cost are reduced in relation to a desired product's actual cost (Monroe 1973; Thaler 1985; Winer 1986; Zeithaml 1988). It also stands to reason that a consumer, when presented with a range of choices for products, is able to compare the choices against each other and select the product which is deemed the most effective. Conversely, traditional fear appeals are typically crafted to offer only one response for the given threat. In the context of information security, if an end user is presented with a range of choices for an effective response to a threat rather than just one response, he or she may feel that the response he or she selects is more effective than others provided, elevating perceptions of response efficacy. Similarly, by offering an end user with choices of effective responses, he or she may also evaluate the costs associated with each of the responses and select the appropriate response based on minimizing cost of performance, thereby decreasing perceptions of response cost.

> *H13: End user perceptions of autonomy will positively influence perceptions of response efficacy.*
>
> *H14: End user perceptions of autonomy will negatively influence response cost.*

Methods

The sampling frame for this study may consist of any person familiar with performing basic tasks on a computer, including students, faculty, organizational end users, or others. To examine the differences that may exist between using control-oriented fear appeals and self-determined persuasive communication techniques, a 2 x 2 experimental design will be used. Within each treatment group, a respondent will be presented with a description of a specific information security threat and a possible remedy for that threat. One group will view a traditional fear appeal, which consists of persuasive communication directed toward threat severity, threat susceptibility, response efficacy, self-efficacy, and response cost. This treatment is designed motivate respondents using only extrinsic means. A second group will be presented with a message designed to appeal to the respondents' perceptions of autonomy, relatedness, and competence related to performing a response behavior, targeting only intrinsic motivation within respondents. The third group will receive a message containing elements of fear appeals as well as appeals toward self-determined variables, thus motivating respondents both extrinsically and intrinsically. The final group will not be presented with any type of persuasive communication, but rather a simple message detailing the nature of the threat (without mention of the severity or susceptibility) and a particular response to that threat (without stating the effectiveness or ease of use related to the recommended response). Because individuals possess a global orientation toward self-determined or control-oriented behaviors, respondents will be randomly selected to treatment groups to partial out any variance in behavioral intention that may be attributed to global-level motivation (Bhattacherjee 2012).

After the respondent has read the treatment message, perceptions of threat and coping variables, behavioral intention, and motivational variables will be measured using a self-report survey. Each scale will be measured using a 5-point fully anchored Likert scale rated from “strongly disagree” to “strongly agree.” Previously validated scales for each construct will be used in this research. Scales for threat severity, threat susceptibility, response efficacy, self-efficacy, and behavioral intention will be adapted from Johnston and Warkentin (2010). Scales for response cost will be adapted from Ifinedo (2011). Scales for autonomy, relatedness, competence, and motivation toward performing the recommended response will be adapted from Vallerand (1997). AMOS 20 will be used to analyze the structural model for model fit and significance of hypothesized relationships. SPSS 21 will be utilized to examine differences between treatment groups based on perceptions of motivation, threat and coping appraisal variables, and behavioral intention using ANOVAs.

Conclusion

Due to inconsistencies in prior applications of PMT in information security contexts, this study could provide insight toward determining other factors that may explain the differences in how individuals experience threat and coping mechanisms related to information security threats when compared to PMT’s native applications, such as health care or driver safety. Examining the differences between traditional fear appeals and intrinsically-focused persuasive communication may also help inform managers in crafting effective appeals that sufficiently influence employees to perform secure behaviors. Information security continues to be a relevant concern for many organizations. This study may help mitigate some of these concerns by providing a theoretically-grounded alternative for managers to more effectively communicate information threats to employees.

REFERENCES

Ajzen, I., and Fishbein, M. 1980. *Understanding attitudes and predicting social behavior*, Englewood Cliffs, NJ: Prentice-Hall.

Baumeister, R. F., and Leary, M. R. 1995. "The need to belong: desire for interpersonal attachments as a fundamental human motivation.," *Psychological bulletin* (117:3), pp. 497–529.

Bhattacherjee, A. 2012. *Social Science Research: Principles, Methods, and Practices*, (2nd ed.) Open Access Textbooks.

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.

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* (32:1), pp. 90–101.

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

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1989. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* (35:8), pp. 982–1003.

Deci, E. L. 1972. "The Effects of Contingent and Noncontingent Rewards and Controls on Intrinsic Motivation," *Organizational Behavior and Human Performance* (8:2), pp. 217–229.

Deci, E. L., and Ryan, R. M. 1980. "The Empirical Exploration of Intrinsic Motivational Processes," in *Advances in Experimental Social Psychology*, L. Berkowitz (ed.), New York: Academic Press, pp. 39–80.

Deci, E. L., and Ryan, R. M. 1987. "The Support of Autonomy and the Control of Behavior," *Journal of Personality and Social Psychology* (53:6), pp. 1024–37.

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.

Gagne, M., and Deci, E. L. 2005. "Self-determination theory and work motivation," *Journal of Organizational Behavior* (26:4), pp. 331–362.

Gross, D. 2013. "Report: Eastern European Gang Hacked Apple, Facebook, Twitter," .

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

Ifinedo, P. 2011. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* Elsevier Ltd, pp. 1–13.

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

Miserandino, M. 1996. "Children Who Do Well in School: Individual Differences in Perceived Competence and Autonomy in Above-Average Children," *Journal of Educational Psychology* (88:2), pp. 203–214.

Monroe, K. B. 1973. "Buyers' Subjective Perceptions of Price," *Journal of Marketing Research* (10:1), pp. 70–80.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior towards IS Security Policy Compliance," in *Proceedings of the 40th Hawaii International Conference on System Sciences*, , pp. 1–10.

Reis, H. T., Sheldon, K. M., Gable, S. L., Roscoe, J., and Ryan, R. M. 2000. "Daily Well-Being: The Role of Autonomy, Competence, and Relatedness," *Personality & Social Psychology Bulletin* (26:4), pp. 419–435.

Richardson, R. 2011. "2010/2011 CSI Computer Crime and Security Survey," .

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The 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 Protected Motivation," in *Social Psychophysiology: A Sourcebook*, J. T. Cacioppo and R. E. Petty (eds.), New York: The Guilford Press, pp. 153–176.

Ryan, R. M. 1982. "Control and Information in the Intrapersonal Sphere: An Extension of Cognitive Evaluation Theory," *Journal of Personality and Social Psychology* (43:3), pp. 450–461.

Ryan, R. M. 1991. "The Nature of the Self in Autonomy and Relatedness," in *The Self: Interdisciplinary Approaches*, New York: Springer, pp. 208–238.

Ryan, R. M., and Deci, E. L. 2000a. "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions.," *Contemporary Educational Psychology* (25:1), pp. 54–67.

Ryan, R. M., and Deci, E. L. 2000b. "Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being," *American Psychologist* (55:1), pp. 68–78.

Ryan, R. M., Mims, V., and Koestner, R. 1983. "Relation of Reward Contingency and Interpersonal Context to Intrinsic Motivation: A Review and Test Using Cognitive Evaluation Theory," *Journal of Personality and Social Psychology* (45:4), pp. 736–750.

Sasse, M. A., Brostoff, S., and Weirich, D. 2001. "Transforming the 'Weakest Link' — A Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal* (19:3), pp. 122–131.

Thaler, R. 1985. "Mental Accounting and Consumer Choice," *Marketing Science* (4:3), pp. 199–214.

Thomson, M. 2006. "Human Brands: Investigating Antecedents to Consumers' Strong Attachments to Celebrities," *Journal of Marketing* (70:3), pp. 104–119.

Vallerand, R. J. 1997. "Toword A Hierarchical Model of Intrinsic and Extrinsic Motivation," *Advances in Experimental Social Psychology* (29), pp. 271–360.

Vallerand, R. J. 2000. "Deci and Ryan's Self-Determination Theory: A View From the Hierarchical Model of Intrinsic and Extrinsic Motivation," *Psychological Inquiry* (11:4), pp. 312–318.

Vallerand, R. J., Fortier, M. S., and Guay, F. 1997. "Self-Determination and Persistence in a Real-Life Setting: Toward a Motivational Model of High School Dropout," *Journal of Personality and Social Psychology* (72:5), pp. 1161–1176.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3-4)Elsevier B.V., pp. 190–198.

Venkatesh, V., and Davis, F. D. 2000. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Management Science* (46:2), pp. 186–204.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425–478.

Venkatesh, V., Thong, J. Y. L., and Xu, X. 2012. "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," *MIS Quarterly* (36:1), pp. 157–178.

Winer, R. S. 1986. "A Reference Price Model of Brand Choice for Frequently Purchased Products," *Journal of Consumer Research* (13:2), pp. 250–256.

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

Zeithaml, V. A. 1988. "Consumer Perceptions Of Price, Quality, and Value: A Means-End Model and Synthesis of Evidence," *Journal of Marketing* (52:3), pp. 2–22.