Routledge
Taylor & Francis Group

Journal of Management Information Systems

ISSN: 0742-1222 (Print) 1557-928X (Online) Journal homepage: http://www.tandfonline.com/loi/mmis20

User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory

Philip Menard, Gregory J. Bott & Robert E. Crossler

User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory

PHILIP MENARD, GREGORY J. BOTT, AND ROBERT E. CROSSLER

Philip Menard (pmenard@southalabama.edu; corresponding author) is an assistant professor of information systems at the University of South Alabama. He received his Ph.D. from the Department of Management and Information Systems at Mississippi State University and is also a past recipient of the CyberCorps Scholarship for Service. He is interested in the impacts of security measures on organizational end users, security education training and awareness (SETA) programs, and the impact of espoused cultural values on individuals' secure behaviors. He has published in *Journal of Management Information Systems, Journal of the Association for Information Systems*, and *Journal of Computer Information Systems*. He has also presented his work at several conferences.

Gregory J. Bott (gjbott@cba.ua.edu) is an assistant professor of information systems in the Culverhouse College of Business at the University of Alabama. He received his Ph.D. from the Department of Management Information Systems at Mississippi State University. He is a recipient of the CyberCorps Scholarship for Service award. His research focuses on information security and privacy. He is a certified digital forensic examiner and serves as an expert witness in civil and criminal cases. He has worked for Microsoft Corporation and served as chief technology officer for three different organizations. He has presented his work at several major conferences.

Robert E. Crossler (rob.crossler@wsu.edu) is an Assistant Professor of Information Systems in the Carson College of Business at Washington State University. He received his Ph.D. from the Department of Accounting and Information Systems at Virginia Tech. His research focuses on the factors that affect the security and privacy decisions individuals make. He has published in leading MIS journals, including *MIS Quarterly, Journal of the Association for Information Systems, European Journal of Information Systems, Information Systems Journal, Decision Support Systems*, and *The DATA BASE for Advances in Information Systems*. He received the 2013 INFORMS Information Systems Society (ISS) Design Science Award for his information privacy work, his paper in The DATA BASE for Advances in Information Systems was recognized as the journal's best paper in 2014, and he received the Journal of Information Systems inaugural Best Paper Award in 2017.

Abstract: Managers desiring to protect information systems must understand how to most effectively motivate users to engage in secure behaviors. Information security researchers have frequently studied individuals' performance of secure

Journal of Management Information Systems / 2017, Vol. 34, No. 4, pp. 1203–1230.
Copyright © Taylor & Francis Group, LLC
ISSN 0742–1222 (print) / ISSN 1557–928X (online)
DOI: https://doi.org/10.1080/07421222.2017.1394083

behaviors in response to threats. Protection motivation theory (PMT) has been used to explain individuals' propensity to engage in voluntary secure behaviors, but the adaptation of this theory has yielded inconsistent results. Motivation as a measurable construct, as derived from self-determination theory (SDT), has never been included in or compared against PMT. In this study, we construct security messages that appeal to individuals' intrinsic motivation, rather than fear, as a way to elicit secure responses. Using three sets of respondents, we integrated the SDT and PMT models and compared the native models in the context of security behaviors. We demonstrate that by using data- and individual-focused appeals and providing choices for users, managers may observe greater intention to engage in secure behavior among employees.

Key words and phrases: information security, protection motivation theory, security model comparison, self-determination theory, user security behaviors.

End users, whether within organizations or in the home-computing context, possess important information that must be protected from various forms of security threats. Home users invest substantial resources in securing their data, including the adoption of antivirus software, antispyware software, identity theft prevention services, and automated cloud-based backup solutions. While having security countermeasures in place is a step in the right direction, home users often fail to adopt secure behaviors on a regular basis (i.e., sharing passwords, using weak passwords, clicking on unfamiliar links, and downloading e-mail attachments without proper scrutiny) [3, 19, 46]. Similarly, in the organizational context, end users are the root cause of approximately 25 percent of data breaches [50]. As a result, organizations make large investments in preventing such breaches because the cost for a data breach reached a record high in 2015 [50] and the confirmed number of data breaches increased by 55 percent [71]. However, many security controls still heavily rely on human intervention. To address this concern, information security (InfoSec) researchers have presented a broad range of studies on the topic of security behaviors.

Protection motivation theory (PMT) has been adapted to better understand what motivates individuals to comply with security policy [32, 33], backup data [13, 42], and employ antimalware software [35, 38]. PMT has also been used to explain multiple behaviors aimed at protecting home computers and networks [4, 15, 75] as well as to explain why users who understand how to protect their systems fail to do so [76].

Although PMT has often been applied in InfoSec research, results have been inconsistent and contradictory. Table A1.1 in Online Appendix A provides a review of InfoSec research using PMT. For each study, the number of observations, sample frame, and results are provided. Study results demonstrate inconsistency in each of the key PMT constructs. While PMT effectively explains the danger control processes leading to message acceptance, the message (fear appeal) in InfoSec research may be misaligned. PMT originated in the context of health care and is predicated on personal threat [25]. Threats to one's health are intrinsically personal. Within InfoSec research, threats are most often against assets that belong to an organization and not directly against individual assets. Because a data breach may or may not have direct consequences for the individual, the breach may lack personal relevance, rendering the cognitive assessment of the threat unnecessary [11, 36]. This inability to trigger the cognitive processes using a fear appeal may also be due to our lack of understanding about the circumstances generating fear in individuals [17]. PMT is predicated on the idea that motivation toward protection stems from a perceived threat and a desire to avoid a potential negative outcome. Motivation arouses, sustains, and directs activity and may influence a user to comply with security policy and take action to protect information assets. Motivation has been heavily studied in both psychology and sociology and has been shown to have significant effects on affect, cognition, and behavior [61], which are also dependent variables that have been studied as critical outcomes in behavioral InfoSec research [17]. Interestingly, PMT is designed to motivate the performance of protective behaviors. However, with the exception of one study, motivation itself has not been included as part of the PMT model in subsequent adaptations for InfoSec research, despite its modeling as a clear outcome in its native discipline (see Figure 1). In the study that included motivation, the authors used behavioral intention measurement items rather than previously validated motivation scales [51]. Motivation has been adapted for information systems in various forms [21, 31, 39, 66, 67], but very few studies have examined motivation in the context of InfoSec as adapted from self-determination theory (SDT) [47, 72, 73, 78]. An application of SDT to InfoSec through the design and use of a self-determined appeal may also fill the relevance gap apparent in many behavioral InfoSec studies. A self-determined appeal is designed to bolster the critical drivers of self-determination to elicit a more internalized motivation in an individual. This research is the first to directly compare the impact of self-determined appeals to the influence of fear appeals.

Using PMT and prior research in motivation as a foundation, this study aims to answer the following research questions:

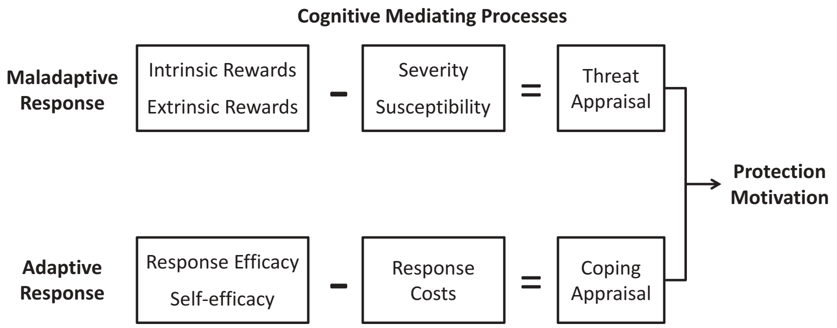

Figure 1. Protection Motivation Theory (Adapted from Floyd et al. [25])

How does the inclusion of an explicit measure of motivation and its key antecedents contribute to the explanation of one's intention to perform secure behaviors?

How does a security appeal driven by self-determination influence individuals' perceptions of threat and coping mechanisms associated with protection motivation?

Literature Review and Hypothesis Development

Protection Motivation Theory

PMT was originally proposed by Rogers [54] and subsequently extended [55] in the health safety and awareness research domain (see Figure 1). PMT theorizes that when an individual is confronted with a threat, he or she cognitively assesses the threat and a possible associated remedy. After conducting threat and coping appraisals, the individual chooses to behave in either an adaptive or maladaptive manner. Adaptive behaviors are recommended responses that are intended to protect someone against the threat, whereas maladaptive responses encompass an array of behaviors in which the threat recipient avoids enacting a recommended response.

The cognitive process of threat appraisal includes the assessment of threat susceptibility, threat severity, and the extrinsic or intrinsic rewards achieved by performing a maladaptive behavior [25, 54]. Threat susceptibility refers to the degree to which someone feels vulnerable to a particular threat. Threat severity is one's perceptions of the seriousness of the threat. Intrinsic rewards refer to the pleasure of committing a maladaptive behavior, whereas an extrinsic reward may be the obtaining of something valuable that could not be feasibly obtained without committing the act. PMT posits that threat susceptibility and severity have positive effects on adaptive behavior and that intrinsic and extrinsic rewards minimize an individual's sensitivity to the threat and have a negative impact on adaptive behavior [49].

Following threat appraisal, an individual conducts an appraisal of available coping mechanisms. Coping appraisal involves the assessment of response efficacy, self-efficacy, and response cost [25, 54]. Response efficacy refers to an individual's perception of how well the recommended response addresses the threat at hand (e.g., follow security policy). Self-efficacy is the confidence an individual possesses in effectively performing the recommended response. Response cost relates to the perceived extrinsic or intrinsic personal costs of performing the suggested adaptive behavior. An individual may interpret response cost in a number of forms, including time, money, or effort. Response efficacy and self-efficacy positively affect intentions to perform adaptive behaviors, whereas response cost negatively affects adaptive behavioral intentions [14, 32, 38]. The outcome of the two cognitive processes is protection motivation, which is "an intervening variable that has the typical characteristics of a motive: it arouses, sustains, and directs activity" [54, p. 98].

PMT has been widely adapted in the field of InfoSec largely due to the common pairs of information threats and effective countermeasures, also known as threat–response pairs, studied in behavioral security contexts. For example, changing and maintaining strong and unique passwords is a response for mitigating the threat of identity theft. Performing data backups is a response for minimizing the threat of data loss [16]. InfoSec's threat–response pairs align well with PMT's cognitive model based on an individual's appraisal of the threat and the recommended coping mechanism. Some widely cited examples of PMT's application in InfoSec include the effect that information quality has on intentions to comply with security policies [48]; the effects of social influence on an organization's attitude toward adoption of antispyware software [38]; and the effect of perceived citizen effectiveness and the collective perceived ownership of the Internet on an individual's motivation to protect the Internet [4] (see Online Appendix A for a complete summary).

Johnston and Warkentin's [35] fear appeal model, in conjunction with key follow-up studies, is possibly the most relevant prior research for the present study. Based on PMT, the authors used a fear appeal to communicate the threat of harmful spyware and the efficacy of an easy-to-use antispyware software to end users. As a result, their research on persuasive communication related to eliciting protective computing behaviors has informed our study of using motivational language in security appeals. However, subsequent work by Johnston et al. [36] and Boss et al. [8] have highlighted both the inconsistencies and misapplication of PMT in InfoSec research. Johnston et al. [36] assert that PMT-based InfoSec appeals lack personal relevance to the end users to whom they are presented. Boss et al. [8] note that very few PMT-based studies have employed experimentally manipulated fear appeal components, while none have explicitly measured fear as a key component of the PMT model. To further investigate these inconsistencies and fill the gap of PMT-based InfoSec research, this study offers a direct comparison of appeals based on PMT against appeals based on SDT, which has been extensively used in psychology and sociology research to explain individuals' motivations [61]. We also aim to fill the gap of actually measuring motivation in relation to security appeals.

Despite the multitude of PMT-based studies conducted in the InfoSec domain, their results have been inconsistent in relation to those derived from PMT's native field of health care [17]. Inconsistencies in InfoSec results could be due to a misspecification of the original PMT model in InfoSec contexts [36]. The crux of the misspecification is the nature of a person's cognitive processes related to individual health care. If a particular threat is directly related to a person's health or well-being, then the threat is perceived as relevant and resonates with the individual. In InfoSec research, threat and coping mechanisms are related to the protection of information belonging to the individual or data with which the individual may interact, creating a phenomenon wherein an individual may be highly motivated to protect some information but may not see the relevance in performing other secure behaviors. For applications centered on organizational rather than personal data, provided a respondent perceives low psychological ownership of the data, the respondents' perception of relevance further decreases [5]. Although the misspecification of PMT in prior InfoSec studies certainly contributes to the described inconsistencies in its adaptation, an entirely different theory may warrant a worthwhile examination as a way to better explain individuals' desire to perform secure behaviors (in Online Appendix A, we provide a detailed tabular summary of PMT's inconsistencies in the InfoSec context).

One factor that may influence a user's intention to perform secure behaviors is motivation. Although protection motivation is included as the outcome of PMT's native cognitive process model [25], subsequent PMT research has assumed PMT's influence on motivation but has not directly measured it. Rather, the model measures constructs that are influenced by motivation and triggered as a response to motivation. The constructs offer evidence of motivation, but none individually or in aggregate provides a means to measure motivation. Behavior or intention (the result of motivation) is typically the dependent variable, while motivation is excluded altogether [14, 25, 27, 28]. In our study, we integrate motivation as an explicit measure, along with its critical antecedents, to fill the gap in explaining individuals' intentions to perform secure behaviors.

Self-Determination Theory

Motivation has often been generally categorized as either intrinsic or extrinsic. An individual can also lack motivation altogether, a state known as amotivation [57]. When an individual experiences *intrinsic motivation*, he or she performs "an activity for itself, and the pleasure and satisfaction derived from participation" [61, p. 279]. When an individual experiences *extrinsic motivation*, he or she is "engaging in an activity as a means to an end and not for its own sake" [61, p. 279]. *Amotivation* is "the lack of intentionality and thus the relative absence of motivation" [61, p. 279]. An example of extrinsic motivation in an InfoSec context is an individual who performs secure behaviors merely because of an organizational mandate. The act of performing secure behaviors purely because of a personal desire to protect organizational information is an example of intrinsic motivation.

Following a number of studies analyzing intrinsic and extrinsic motivation as dichotomous, Deci and Ryan [22] proposed SDT, which identifies discrete types of extrinsic motivation, each with distinct levels of self-determined, or autonomous, origins. This means that extrinsic motivation is categorized by the degree to which an individual's motivation is controlled by some external entity [80]. *External regulation*, which is the least self-determined form of extrinsic motivation, refers to regulating an individual's behavior purely by external means, such as rewards (i.e., money) or constraints (i.e., sanctions). *Introjected regulation* occurs when an individual internalizes the reasons for his or her actions, meaning the motivation is internal but not self-determined (i.e., praise or shame offered by important others). *Identified regulation* occurs when behavior is highly valued and judged as important upon identification (i.e., the behavior is simply a means to some self-determined end). *Integrated regulation* refers to an externally derived behavior that has been fully internalized by the individual, meaning that an individual's choices are made as an extension of the self (i.e., performing an unpleasant but necessary work-related behavior because an individual sees himself as a good employee).

Additionally, SDT theorizes that an individual's self-determined motivation is influenced by perceptions of autonomy, competence, and relatedness [22]. SDT refers to *autonomy* as one's perception of the degree to which he or she may engage in activities of his or her own desire. *Competence* is defined as the degree to which an individual feels he or she can interact effectively with his or her surroundings 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 [63]. Using an employee as an example, the employee may perceive high levels of autonomy, competence, and relatedness if he feels he has the freedom to conduct his daily tasks in the manner he chooses, confidence in his ability to achieve his work-related goals, and a friendly rapport with his coworkers.

Although autonomy, competence, and relatedness have demonstrated a positive effect on motivation, researchers studying persuasive communication related to security threats have mainly examined the prompting of secure behavior through the use of fear appeals, which are focused on control-oriented motivational techniques [35, 48, 77]. When presented with a fear appeal, individuals may feel they are being prompted to perform a behavior that is not self-determined, based on the threat's origination with an external entity. Embedding autonomy, competence, and relatedness in a security appeal may bolster individuals' perceptions of intrinsic motivation and may subsequently influence an end user's performance of secure behaviors.

Hypothesis Development

Given the similarities in PMT and SDT with regard to explaining behavioral intentions in the presence of motivation, it is theoretically plausible and statistically possible to test a combined model that includes both sets of constructs. Doing so requires establishing the nature of the combined model, at which point a comparison can be made to the original models. Specifically, the embedded manipulations of relatedness, competence, and autonomy in security appeals (as described later) may influence not only motivation and intention but also the PMT variables. Our hypotheses related to the combined model are illustrated in Figure 2 and described in greater detail below.

One of the consistent issues with the adaptation of PMT to the InfoSec context is the potential for someone to perceive threats to their information as irrelevant [17]. The perceived lack of relevance occurs during the threat appraisal process. If the target of the threat is irrelevant to an individual, he or she will ignore the threat, regardless of its severity or his or her susceptibility. Relatedness, from SDT, in this context refers to an individual's emotional connection to his or her data. Within the home environment, the emotional connection to data is straightforward. However,

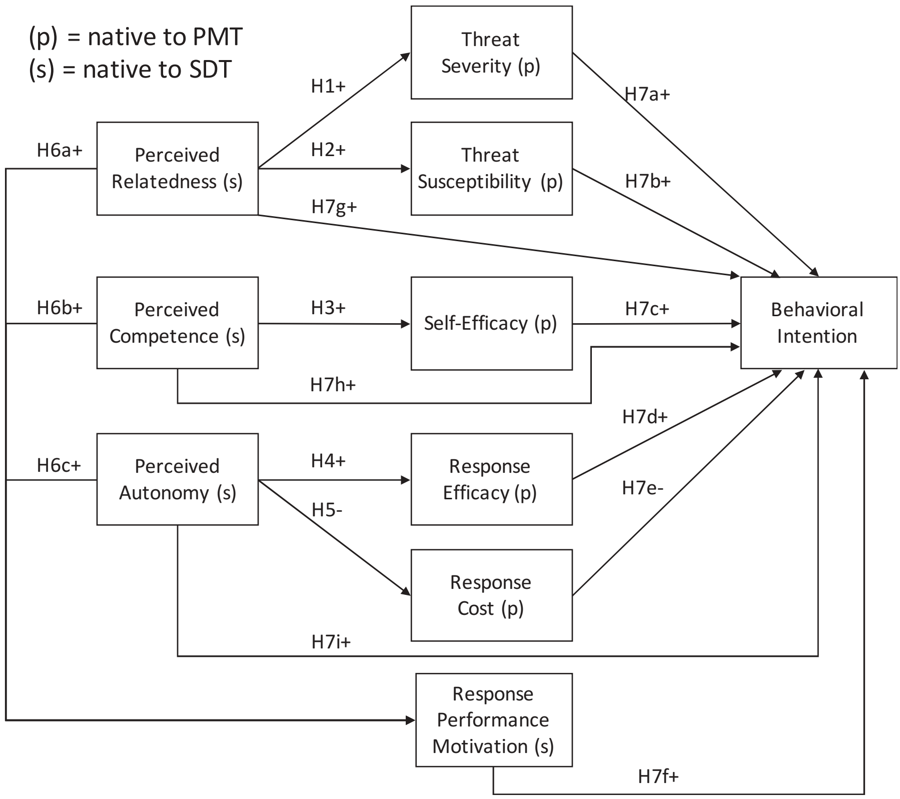

Figure 2. Integrated Model of SDT and PMT for Security Appeal Perceptions

individuals may also have a strong emotional connection to data in the organizational context. The loss of organizational data may represent work stoppage, embarrassment, missed deadlines, or a significant amount of rework (even if data are restored). Relatedness can establish the relevance of the threat by emphasizing the emotional connection between the individual and his or her data. When a connection to one's information occurs at an emotional level, one's perceptions of the threat will resonate. 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 as elevated. For example, a photograph taken of scenery during a vacation may not contain personally identifiable information, but a threat to that photograph may be perceived as severe due to an individual's relatedness toward the photo. Similarly, if an individual feels a connection with the data being protected, he or she may also feel more susceptible to the threat, regardless of the actual mathematical probability of the threat occurring. Based on these arguments, we present the following hypotheses:

> *Hypothesis 1: Perceived relatedness will positively influence perceptions of threat severity.*

Hypothesis 2: Perceived relatedness will positively influence perceptions of threat susceptibility.

Competence as studied in motivational research and within SDT refers to an individual's confidence in his or her ability to learn about and execute a range of tasks within a given domain. In this context, an individual's competence is related to security-focused tasks carried out on a computing device. Competence is conceptually 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 [25, 55]. The generality of competence and the specificity of self-efficacy necessitates that they are theoretically distinct constructs, but their conceptual similarity indicates that a relationship may exist between them. If an end user perceives a high degree of confidence in performing activities related to securing information, the end user should feel confident in his or her ability to learn how to perform a variety of security-based actions and thus will experience an increase in self-efficacy with regard to performing the particular recommended response communicated in the appeal.

Hypothesis 3: Perceived competence will positively influence perceptions of self-efficacy.

Autonomy, from SDT, has been shown to have a powerful influence on individuals' perceptions of intrinsic motivation [40, 58, 61, 62]. 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 [23, 26, 43, 52]. 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 [44, 59, 74, 79]. It also stands to reason that a consumer, when presented with a range of product choices, is able to compare the choices against each other and select the product that 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 InfoSec, if an end user is presented with a range of effective responses to a threat rather than just one choice, he or she may feel that the response he or she selects is more effective than other provided options, elevating perceptions of response efficacy. Similarly, by offering an end user multiple 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.

Hypothesis 4: Perceived autonomy will positively influence perceptions of response efficacy.

Hypothesis 5: Perceived autonomy will negatively influence perceptions of response cost.

According to SDT [22], an individual's degree of self-determined motivation may be affected by his or her perceptions of relatedness, competence, and autonomy. Using Vallerand's hierarchical model [61] as a basis, we are examining motivation at the situational (i.e., task-specific) level of an individual's motivation to perform a security-related task. This means that the critical factors that will influence an individual's motivation to perform a recommended response will be security-related forms of relatedness, competence, and autonomy. These factors are adapted for the information security context to examine the internalization of individuals' motivation to perform secure tasks.

Typically, relatedness in motivational research refers to the degree of connectedness an individual feels toward others when interacting in a specific context, such as school or work [58, 61, 62]. 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 [6, 60]. 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. In motivational research, competence refers to the level of confidence an individual perceives in a particular range of activities in which he or she is engaged [22]. For this research, competence is related to the level of confidence an individual perceives toward learning about and executing security-related tasks. Autonomy refers to the self-regulation of behavior and the degree of governance one experiences toward the initiation and direction of his or her actions [56]. Here, autonomy is the degree of freedom an individual perceives in relation to decisions made regarding recommended responses to security threats.

If an individual feels a strong sense of connection to the information being protected, his or her motivation to perform the response 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 an increased degree of autonomy related to the types of recommended responses available to mitigate the threat, his or her motivation will also become more self-determined. These hypotheses align with numerous studies regarding SDT, but they must still be validated in the context of information security and the use of fear appeals. Thus, we offer the following hypotheses:

Hypothesis 6a: Perceived relatedness will positively influence motivation toward performing the recommended response.

Hypothesis 6b: Perceived competence will positively influence motivation toward performing the recommended response.

Hypothesis 6c: Perceived autonomy will positively influence motivation toward performing the recommended response.

Prior work in PMT research has established that threat and coping appraisals form an individual's protection motivation, which is a specific type of motivation driven by the fear of an impending threat [25]. In our study, we present an alternative type of motivation driven by an individual's self-determined desire to perform protective actions regardless of fear—response performance motivation. In the extant literature related to self-determination, motivation is depicted as having a direct effect on behavior [61]. In prior PMT-related research, the variables used to constitute protection motivation (threat severity, threat susceptibility, response efficacy, self-efficacy, and response cost) are depicted as having a direct effect on behavior [25]. In both streams, specific types of motivation influence behavior or intention but are clearly separate forms of motivation. We maintain this distinction in our model, which includes protection motivation factors and variables representing self-determination. For this reason, we do not hypothesize any relationships between the PMT variables constituting protection motivation and response performance motivation.

The next nine hypotheses represent the independent variables of the traditional PMT model and SDT model and the influence of those variables on behavioral intention. While the remaining hypotheses are not novel in InfoSec, PMT, or SDT research, testing boundary conditions, including the native established relationships, is necessary for theory adaptation and contextualization [28, 29]. Although we are not conducting a replication study, we have tested the relationships for our adaptation of PMT to the context of self-determined appeals.

A critical aspect of protection motivation theory is the presumption that an individual initiates a cognitive process to evaluate a particular threat, in terms of both severity and the likelihood of such a threat affecting that person [25, 54]. These relationships have been posited throughout the existence of PMT, and extensive empirical evidence supporting these hypotheses has been presented in prior research [25, 32, 48]. Thus, the following hypotheses are presented:

> *Hypothesis 7a: Perceived threat severity will positively influence behavioral intention to perform secure behaviors.*

> *Hypothesis 7b: Perceived 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 intentions to perform secure behaviors. After cognitively processing the attributes of an existing threat, the individual conducts another cognitive assessment regarding the 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 [55]. As the cost of performing the response, which may be composed 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 using PMT [25, 35, 77]. Likewise, we present the following hypotheses:

Hypothesis 7c: Perceived self-efficacy will positively influence behavioral intention to perform secure behaviors.

Hypothesis 7d: Perceived response efficacy will positively influence behavioral intention to perform secure behaviors.

Hypothesis 7e: Perceived response cost will negatively influence behavioral intention to perform secure behaviors.

According to Vallerand's hierarchical model of motivation [61], one of the outcome variables of motivation is behavior. However, many studies in social psychology have examined the relationship between intentions and behavior and have found that the formation of intentions precedes the performance of the actual behavior [1]. Adaptations of intention to perform a behavior have been widely used in information systems research [20, 68, 69, 70] as well as specifically in information security research [10, 18, 32, 35]. An individual who is intrinsically motivated to perform a secure behavior should consequently form intentions to execute that response. Thus, we hypothesize the following:

Hypothesis 7f: Motivation toward performing the recommended response will positively influence behavioral intention to perform secure behaviors.

Prior motivational studies have shown that autonomy, competence, and relatedness are critical factors that influence an individual's self-determined motivation [61]. Various research on motivation has also demonstrated that these key variables individually have positive direct effects on behavior. Impeding any one of these critical factors would ultimately result in decreased likelihood of performing a recommended behavior. By crafting an appeal that bolsters these perceptions (see further explanation of security appeals under Sampling Frame and Appeal Contextualization), we expect to see positive effects on intention as well. As one's perception of relatedness increases, intentions to perform a recommended secure behavior may also increase due to the emotional connection perceived toward the data at risk. As one's perception of competence increases, intentions to perform secure behaviors may be elevated due to the individual's increased confidence in learning about and understanding the threat. As one's perception of autonomy increases, intentions to perform secure behaviors may be more likely because of the increased perceived degree of control of the user regarding the threat's countermeasure. Based on these arguments, we present the following hypotheses:

Hypothesis 7g: Perceived relatedness will positively influence behavioral intention to perform secure behaviors.

Hypothesis 7h: Perceived competence will positively influence behavioral intention to perform secure behaviors.

Hypothesis 7i: Perceived autonomy will positively influence behavioral intention to perform secure behaviors.

Further Investigation of Motivational Processes in Information Security Contexts

An additional goal of this research is to examine the effectiveness of the specific statements included in security appeals. In prior arguments, we hypothesize that motivation and its antecedents represent significant and necessary components of individuals' perceptions of InfoSec threats and their formulation of intentions to perform secure behaviors. Although we are proposing an integration of SDT- and PMT-related perceptions in a single model, direct comparisons between PMT and SDT may further highlight the importance of self-determined motivation in security appeal contexts. Building on the relationships examined in the previous hypotheses, we provide additional analysis of the nature of motivational processes in InfoSec contexts in the following arguments (see Data Analysis and Results section).

Method

Research Design

To examine the influence of SDT-based security appeals on individuals' security perceptions as well as the differences that exist between PMT and SDT in terms of their effectiveness in explaining security behaviors, we used a full factorial experimental design [12, 64], embedding either SDT-based or PMT-based messages in security-focused appeals. Within each appeal, a respondent was presented with a random combination of statements, where each statement is designed to bolster the end user's perception of the independent variables pertinent to either SDT or PMT. Because the integrated SDT–PMT model includes relationships that position autonomy, competence, and relatedness as independent variables influencing PMT variables, respondents included in the analysis of the integrated model were shown the SDT-based appeal. This design allowed us to examine the variance in the PMT variables that can be explained by the SDT manipulations in the appeal. SDT is composed of three independent variables (autonomy, competence, and relatedness); thus, there are three possible SDT-based manipulation statements that may be embedded in the SDT-based appeal. This appeal design results in 2^3, or 8, possible combinations of statements to be embedded in the SDT-based appeal.

Because this study was also designed to compare the native PMT and SDT models directly, we also designed a traditional PMT-based appeal with manipulation statements directly tied to the PMT variables. As PMT is composed of five independent variables (threat severity, threat susceptibility, response efficacy, self-efficacy, and response cost), a full factorial manipulation of a PMT-based appeal results in 2^5, or 32, possible statement combinations in the PMT-based appeal. PMT- and SDT-based appeals remained isolated from one another in our manipulations (i.e., a respondent receiving a PMT-based appeal could receive any combination of PMT-based statements but would not receive any SDT-based statements). Each respondent was exposed to only one security appeal. Our sample consisted of three subsets: (1) respondents who were presented the SDT-based appeal and included in analysis of the integrated SDT–PMT model; (2) respondents who were presented the SDT-based appeal and included in the model comparison analysis of SDT and PMT; and (3) respondents who were presented the PMT-based appeal and included in the SDT–PMT model comparison. Further description of our sampling frame and appeal context is provided next.

Sampling Frame and Appeal Contextualization

Although motivation may play an important role in the performance of secure behaviors in both home and organizational contexts, we considered a tight research design to be paramount for our research considering our inclusion of an important construct (motivation) that has previously been excluded from behavioral security research. SDT and PMT are both individual-based theories that may drive behavior, whether the individual is a home user or an employee. However, in the organizational context, a multitude of additional variables external to SDT and PMT may influence individuals' perceptions and conflate potential findings. We decided that because our research includes critical theory-testing hypotheses and direct comparisons of two competing theories [7], the home context would be the most appropriate sampling frame for our current work by offering the purest context for studying these foundational constructs. Building on our study, we recommend further testing in the organizational context, but employees as a sampling frame is outside the scope of the theory testing in the present study.

Because we are analyzing the efficacy of security appeals for end users who are not governed by organizational policies outlining appropriate and secure behavior on their computers, the appropriate respondent for our study was an end user who owned a home computer for personal use and was also the primary decision maker for installing software on the machine. Mindful that many end users already possess baseline knowledge regarding common security threats, such as viruses or spyware, and have probably already decided on an appropriate software solution to install, we crafted an appeal that focused on a security countermeasure that has not yet achieved ubiquitous usage. Accordingly, we chose the installation of password management software as the focal security countermeasure in our appeal (see Online Appendix B for a detailed example of our appeal construction).

Although the adoption rate of password managers remains relatively low [2], password managers have been widely recognized as important components of overall security solutions [9] and have been outlined as such by policy guidelines compiled by security professionals [41]. In many cases, strong passwords are the first line of defense against cyber attacks, and research has shown that having a mechanism for managing passwords significantly increases the complexity and security of passwords [37]. We solicited respondents from Amazon Mechanical Turk (MTurk). Our respondents consisted of individuals familiar with performing basic tasks on a computer and who also did not already have password management software installed on his or her personal computer.

Instrument Design

First, the respondent was asked whether he or she already had password management software installed on his or her machine. If the respondent answered “yes,” the respondent was excluded from the remainder of the research. Respondents who answered “no” were presented with either the PMT- or the SDT-based treatment appeal, which randomly included any or all (or none) of the embedded appeal statements representing the PMT and SDT variables. After the respondent read the treatment appeal, the respondent reported the likelihood that he or she would install password management software using a 10-point slider scale, where 10 is “extremely likely” and 0 is “not likely at all.” Following the slider scale, perceptions of threat, coping, and motivational variables were measured using a self-report survey. Each scale was measured using a 5-point fully anchored Likert-type scale rated from “strongly disagree” to “strongly agree.” Previously validated scales for each construct were used in this research. Scales for threat severity, threat susceptibility, response efficacy, and self-efficacy were adapted from Johnston and Warkentin [35]. Scales for response cost were adapted from Ifinedo [33]. Scales for autonomy, relatedness, competence, and motivation toward performing the recommended response were adapted from Vallerand [61]. After respondents answered these measurement items, we presented them with demographic questions, including age, gender, ethnicity, and years of computing experience (see Online Appendix C for a full list of instrument items).

Measuring Motivation

The scale for motivation toward performing the recommended response is designed as a series of multi-item reflective scales assessing types of motivation along the self-determined spectrum. In measuring motivation while a specific activity is being performed or considered, only four types of motivation are assessed for the sake of brevity and to accurately capture the respondent’s motivation in the moment. Adapted from Vallerand’s [61] situational motivation scale, our response performance motivation scale is composed of scales representing intrinsic motivation, identified regulations, external regulations, and amotivation. In line with standard practices from psychology research [61], a composite score representing the respondent’s level of response performance motivation was calculated based on mean scores for each type of motivation. Each item in the scale is measured using a fully anchored 5-point Likert-type scale, and values for the composite motivational score ranged from 1 to 5.

Power Analysis and Data Collection

To determine the minimum sample sizes required for our study, we conducted power analyses using G*Power [24]. For our PMT-based sample, we used values of alpha = 0.05, power = 0.8, number of groups = 32, and estimated effect size = 0.25; we further determined that we needed a minimum sample of 448 to achieve adequate power for statistical interpretation. For our SDT-based sample, we used values of alpha = 0.05, power = 0.8, number of groups = 8, and estimated effect size = 0.25, and we determined that we would need a minimum sample of 240 to achieve adequate statistical power. We collected a total of 1,732 samples from MTurk. Of these, 348 respondents reported that they already had a password manager installed on their computer and thus were not included in the remainder of the study. We then eliminated 52 respondents due to either unreasonably fast completion times or failed attention filter questions (i.e., "For this statement, please answer disagree") that were embedded among our instrument items. Our final sample for analysis of the integrated SDT–PMT model consisted of 547 responses. Our final sample for analysis of the comparison between the SDT and PMT models consisted of 785 total responses (449 who were shown the PMT-based appeal; 336 who were shown the SDT-based appeal).

Data Analysis and Results

This portion of the study explains the data analysis techniques used and analysis of the conceptual model. A detailed description of our data set's validity, including demographic information, instrument validity assessment, and construct validity tests are given in Online Appendix D. Results are further illustrated in model and tabular presentations.

Because our model features a formative construct (response cost) alongside reflective constructs, partial least squares (PLS) analysis is the most appropriate analysis mechanism for the structural model [30]. We chose to analyze the structural model and its associated hypotheses using SmartPLS [53]. A bootstrapping resampling technique, which approximates the path coefficients and the amount of variance explained in mediating variables, was used. Twelve hypotheses were supported, and five were not (see Table 1). The overall findings for hypothesis support are shown in Figure 3. The model explains 54.8 percent of the variance in intention to install password management software. The integration of SDT variables affecting the PMT model also explains 41.3 percent of the variance in threat severity, 13.2 percent of the variance in threat susceptibility, 6.6 percent of the variance in self-efficacy, 37.6 percent of the variance in response efficacy, and 12.3 percent of the variance in response cost. Relatedness, competence, and autonomy collectively explained 39.9 percent of the variance in motivation to perform the recommended response.

In examining the individual relationships in the model, we began with the paths related to the integration of SDT and PMT, analyzing the relationships between our motivational antecedents (relatedness, competence, and autonomy) and the

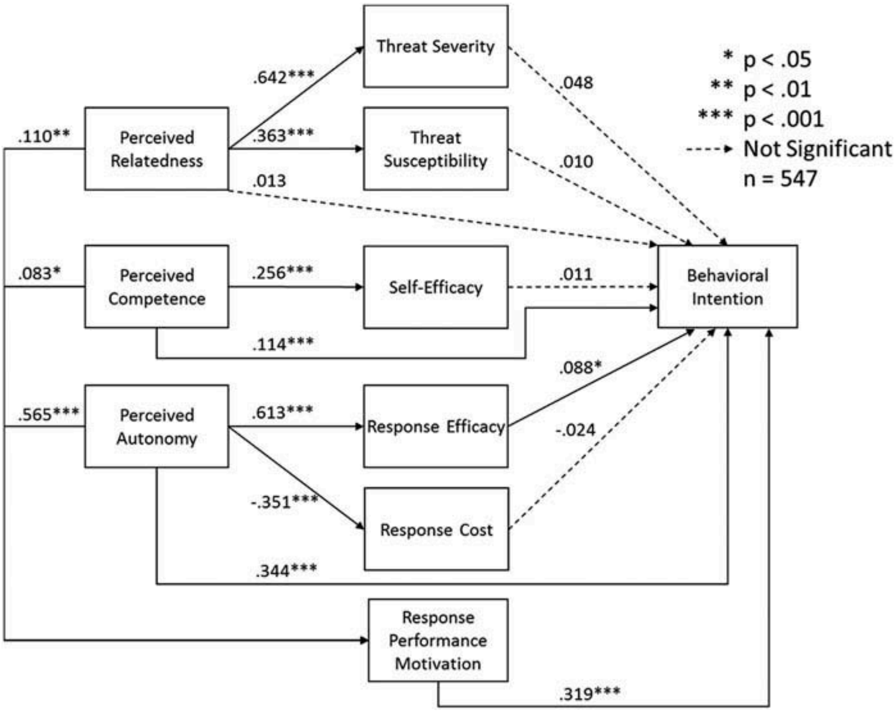

Figure 3. Integrated SDT–PMT Model with Path Significance

traditional PMT variables. Relatedness had a significant positive effect on threat severity (β = .642, *p* < .001) and threat susceptibility (β = .364, *p* < .001). Competence showed a significant positive influence on self-efficacy (β = .256, *p* < .001). Autonomy demonstrated a significant positive effect on response efficacy (β = .613, *p* < .001) and a significant negative influence on response cost (β = −.351, *p* < .001). While traditional fear appeals have been shown to bolster PMT's native variables, the design of a security appeal with statements enhancing perceptions of relatedness, competence, and autonomy, as adapted from SDT, further reinforces individuals' perceptions of the PMT variables in addition to eliciting an intrinsic desire to protect data.

Next, we examined the impact of motivation on intention, as well as the effect of relatedness, competence, and autonomy on motivation. An individual's motivation to perform the appeal's recommended response had a positive significant influence on the individual's intention to perform the response (β = .457, *p* < .001). Embedding motivational enhancements in the appeal for password management software installation bolstered individuals' perceptions of relatedness, competence, and autonomy, either individually or in tandem, depending on the treatment group. As predicted in the research model, individuals' motivation to perform the appeal's recommended response became more self-determined as individuals' perceptions of relatedness (β = .110, *p* < .01), competence (β = .084, *p* < .05), and autonomy (β = .565, *p* < .001) increased. This

Table 1. Path Estimates—Integrated Model

Hypothesis (with direction)	Path coefficient (β)	*t*-statistic	*p*-value	Supported?
H1: REL → TSEV (+)	0.642	21.298	< .001	Yes
H2: REL → TSUS (+)	0.363	9.101	< .001	Yes
H3: COMP → SEF (+)	0.256	5.397	< .001	Yes
H4: AUTO → REF (+)	0.613	19.059	< .001	Yes
H5: AUTO → COS (–)	–0.351	7.568	< .001	Yes
H6a: REL → MOT (+)	0.110	3.059	< .05	Yes
H6b: COMP → MOT (+)	0.083	1.934	< .05	Yes
H6c: AUTO → MOT (+)	0.565	16.821	< .001	Yes
H7a: TSEV → BI (+)	0.048	1.436	> .05	No
H7b: TSUS → BI (+)	0.010	0.308	> .05	No
H7c: REF → BI (+)	0.011	0.305	> .05	No
H7d: SEF → BI (+)	0.088	2.185	< .05	Yes
H7e: COS → BI (–)	–0.024	0.572	> .05	No
H7f: MOT → BI (+)	0.319	7.334	< .001	Yes
H7g: REL → BI (+)	0.013	0.356	> .05	No
H7h: COMP → BI (+)	0.114	3.603	> .05	No
H7i: AUTO → BI (+)	0.344	7.242	< .001	Yes

Notes: IV = Independent Variable; DV = Dependent Variable; BI = Behavioral Intention; MOT = Motivation toward performing recommended response; REL = Perceived Relatedness; COMP = Perceived Competence; AUTO = Perceived Autonomy; TSEV = Threat Severity; TSUS = Threat Susceptibility; REF = Response Efficacy; SEF = Self-efficacy; COS = Response Cost.

finding indicates that each antecedent is individually significant in improving an individuals' self-determined motivation to perform a recommended response.

Finally, we analyzed the paths adapted from the traditional PMT model, along with the direct effects on intention of motivation, relatedness, competence, and autonomy. With the exception of response efficacy ($\beta = .088$, $p < .05$), each of the remaining PMT variables did not significantly influence behavioral intention. Threat severity ($\beta = .048$, $p > .05$), threat susceptibility ($\beta = .010$, $p > .05$), self-efficacy ($\beta = .011$, $p > .05$), and response cost ($\beta = -.024$, $p > .05$) each failed to demonstrate a significant direct effect on an individual's intention to install password management software. Although relatedness did not significantly influence intention ($\beta = .013$, $p > .05$), motivation ($\beta = .319$, $p < .001$), competence ($\beta = .114$, $p < .001$), and autonomy ($\beta = .344$, $p < .001$), each demonstrated significant effects on intention.

Ordinary Least Squares Regression Analysis of Differences Between Self-Determination Theory and Protection Motivation Theory Models

To statistically assess the differences in the amount of variance explained between our competing models, we conducted a series of *F*-tests measuring differences in the models' residual sum of squares and degrees of freedom. In each of our four hypothesized comparisons, the juxtaposed models possess a differing number of independent variables and therefore differing degrees of freedom. To adjust for this, we followed the process outlined by Motulsky and Ransnas [45] in calculating the *F*-statistic with different degrees of freedom. Although it is a simple matter to compare whether one R^2 value is larger than another, by using the formula of Motulsky and Ransnas [45] we can determine whether that difference is significant. Additionally, we are able to detect significant differences based on both the amount of variance explained in the dependent variable and the number of independent variables included in competing models, accounting for model parsimony [45]. A summary of our hypothesis tests and the associated values used for *F*-statistic computation are shown in Table 2.

Comparison of Appeal Manipulation Effects on Intention

First, we compared the traditional PMT model against a model consisting of perceived autonomy, competence, and relatedness. The traditional PMT model included five independent variables and explained 33.5 percent of the variance in behavioral intention. The model featuring only autonomy, competence, and relatedness explained 42.2 percent of the variance in behavioral intention. We observed a significant difference between models ($F = 1.432$; $p = .008$), demonstrating that an appeal including SDT-derived statements explained more variance in intention and did so using fewer independent variables.

Comparison of Appeal Manipulation Effects on Response Performance Motivation

Next, we analyzed the differences between our PMT and SDT appeals based on their impact on motivation to perform a recommended response. PMT's independent variables explained 38.0 percent of the variance in motivation, while SDT's variables explained 37.9 percent of motivation's variance. Because the *F*-test comparison is

Table 2 Model Comparison Results Using *F*-tests

	Model 1				Model 2					
Comparison	SS_R	*n*	IVs	R^2	SS_R	*n*	IVs	R^2	*F*-stat	*p*
PMT→BI vs. SDT→BI	2,090.565	449	5	.335	1,415.027	336	3	.422	1.432	.008
PMT→Mot vs. SDT→Mot	92.912	449	5	.380	63.442	336	3	.379	1.394	.013
PMT→BI vs. PMT+Mot→BI	2,090.565	449	5	.335	1,705.293	449	6	.458	82.862	<.001
PMT+Mot→BI vs. SDT+Mot→BI	1,705.293	449	6	.458	1,183.636	336	4	.515	1.318	.033

Notes: SS_R = Residual Sum of Squares; n = sample size; IVs = number of independent variables; R^2 values reported are adjusted R^2

sensitive to the number of independent variables included in a model and accounts for model parsimony, significant differences between models may be observed even in cases where the amount of variance explained does not differ a great deal between models. Although the SDT and PMT models generate roughly the same R^2 in motivation, the PMT model includes five independent variables whereas the SDT model features just three. A significant difference was observed between our models in terms of SDT being the more parsimonious model ($F = 1.394$; $p = .013$), demonstrating that SDT outperforms PMT in explaining motivation.

Effect of Including Response Performance Motivation in Protection Motivation Theory

Our next comparison examined the difference between the traditional PMT model's effect on intention and a modified PMT model that also included response performance motivation as an independent variable affecting intention. Although the augmented PMT model is not as parsimonious as the traditional model (six independent variables instead of five), it explains a significantly greater amount of variance in intention ($F = 82.862$; $p < .001$).

Comparison of Self-Determination Theory to Modified Protection Motivation Theory

Our final assessment compared the modified PMT model (response performance motivation included) with a modified SDT model (direct effects on intention from autonomy, competence, relatedness, and response performance motivation). The modified SDT model explained a greater amount of variance in intention (51.5 percent) than did the modified PMT model while achieving greater parsimony ($F = 1.318$; $p = .033$).

Discussion

Research Contribution

Our study offers interesting insights into adaptation of theories for InfoSec research, application of motivational research in InfoSec contexts, and differences in security appeals based on fear arousal and intrinsic motivation. Implications for theory and practice are discussed below.

Contribution to Theory

Perhaps most critically, our work offers insight toward explaining the inconsistent results obtained when applying PMT in InfoSec contexts. Motivation has demonstrated a significant influence on both behavioral intention and behavior across numerous studies and research contexts [61]. Thus far, research using PMT as the foundational model has excluded an individual's motivation as a construct. In health care, an individual's motivation to protect him- or herself is apparent, but in InfoSec contexts, an individual's motivation to perform a recommended response is not as evident and may depend on the influence of other factors. By embedding statements focused on enhancing autonomy, competence, and relatedness in our security appeal, we observed that these statements play an important role in enhancing not just their intended independent variables but also those associated with PMT. Bolstering an individual's relatedness increases the relevance of the threat from the perspective of the end user. Reinforcing an individual's competence related to computer-based activities increases the end user's confidence in his ability to enact the recommended response. Strengthening an individual's autonomy increases the end user's confidence in the efficacy of the response and lowers perceived costs related to performing the response. By incorporating SDT into the traditional PMT model, we have introduced key factors that help bridge the gap in adapting PMT for InfoSec research applications.

In addition to SDT's pertinent independent variables, we also included motivation as a construct in our model, in the form of response performance motivation. Our research demonstrates that a measure of motivation, as executed by incorporating SDT, is needed for adapting PMT in InfoSec research contexts to account for an individual's varying motivation to perform a behavior intended to protect information rather than oneself. Prior to this study, there had not been a clear demonstration of whether an explicit measure of motivation, in concert with PMT's traditional independent variables, would have a significant impact on an individual's intention to perform a desired security behavior. Our research shows that response performance motivation contributes substantially to the amount of variance in intention that can be explained by the model. Based on the explanatory findings demonstrated by our results, an explicit measure of motivation should be included in subsequent research related to one's motivation to perform protective behaviors on one's data.

The development of our integrated model also allowed for a mediation analysis to be conducted (see Online Appendix E). This examination helped us gain a more complete understanding of the nomological network of key motivational variables in InfoSec contexts. Response performance motivation partially mediated the relationship between competence and intention, as well as the relationship between autonomy and intention. Motivation fully mediated the relationship between relatedness and intention. This finding helps fill an important gap in identifying how to incorporate personal relevance when influencing individuals to perform secure behaviors. Relatedness, or the emotional connection between individuals and their data, did not directly affect intention but was an important factor in driving motivation to perform secure behaviors. If motivation had been left out of the model, relatedness would have appeared to be a nonsignificant factor, while that was not actually the case. The indirect effect of relatedness on intention is thus a key finding. The nature of this relationship again highlights the importance of including an explicit measure of motivation in future research studying motivational processes regarding secure behaviors.

By empirically comparing PMT to SDT in InfoSec applications, we have demonstrated that SDT explains a significantly greater amount of variance in intention to perform a secure behavior while also doing so more parsimoniously than PMT. With only three independent variables, SDT offers a more efficient means of predicting end users' intention to perform secure behaviors. A more parsimonious model for designing security appeals also leads to shorter, more tightly constructed appeals, easing the burden on end users' cognitive load. Efficiently persuading end users to perform a recommended response is paramount in formulating intentions, and eventually, behaviors. Our research also highlights a novel adaptation of SDT for InfoSec applications. By developing self-determined appeals based on bolstering end users' autonomy, competence, and relatedness through persuasive communication, we have shown that SDT offers a unique perspective on human behavior previously unexplored in InfoSec research.

An interesting outcome of our analysis was the shifting strength of the influence of response efficacy and self-efficacy toward intention. InfoSec-based studies using PMT have often shown that self-efficacy is the most important factor in explaining individuals' intention to perform a recommended response [17]. Rather, our data show that response efficacy is the strongest of the traditional PMT independent variables, second overall only to response performance motivation, in explaining the variance of an end user's intention to install a password manager. This finding may speak to the continually evolving skills possessed by our targeted end users. Most end users are comfortable installing and using software on their machines [65]. End users may be more interested in how well the recommended solution handles the problem at hand. They may also desire to learn about the options available to them and select their preferred response from a variety of alternatives. A model that incorporates SDT is more robust in communicating an effective range of options through its autonomy-based statements in the appeal.

Contribution to Practice

By comparing the efficacy of PMT-based appeals to that of SDT-based appeals, we have demonstrated that an appeal that is more data- and individual-focused, rather than fear- or threat-focused, is more effective at forming intentions to perform a recommended response and reinforces an end user's intrinsic desire to protect his information. Prior adaptations of fear appeals in InfoSec contexts assumed relevance to the end user and relied on fear as the main motivator [36]. However, if a threat is irrelevant, then the appeal does not arouse fear, fails to resonate with the end user, and will not be adequately internalized. InfoSec professionals should consider developing security appeals that bolster end users' perceptions of autonomy, competence, and relatedness. With carefully crafted motivational appeals, security professionals should observe an increase in end users' intention to protect information as described in the appeal.

Autonomy was an especially strong factor in our self-determined appeals. The strength of the autonomy manipulation was especially pronounced in users' perceptions of response efficacy. InfoSec professionals should also note the increased importance of response efficacy in the InfoSec-adapted PMT model. By offering end users a range of viable options for protecting their information, we were able to elicit perceptions of choice among our respondents, allowing them to select an appropriate response according to their preferences. Although organizational end users are typically mandated to install and use certain software solutions, home computer users have complete control of their machines and value freedom of choice. Practitioners charged with creating security appeals should consider incorporating an element of choice in security appeals designed for home computer users.

Limitations and Future Research

Despite our best efforts to mitigate weaknesses in our study's design, our research is not without limitations. Several secure behaviors have been analyzed using security appeals, but our study featured just one recommended behavior: the installation and use of a password manager, which was selected due to its current low adoption rate. While our findings are insightful for PMT adaptations and overall behavioral InfoSec research, retesting our appeals using a variety of other behaviors, such as performing data backups or using antivirus software, may highlight interesting differences. Researchers may elect to study just one behavior or craft several different appeals focusing on single specific behaviors.

A related limitation is our use of intention rather than actual behavior as our dependent variable. Although the primary goal of our research was to position SDT as a suitable alternative foundational theory for behavioral InfoSec, and our focus on intention was driven by prior work in PMT, many scholars have noted the issues inherent in using intention as a proxy for behavior [17, 34]. Future research may further test our findings by using a measure of actual behavior in tandem with an intention scale.

Although we focused our appeals toward home users in our research design, our self-determined appeal and integrated SDT-PMT model is applicable to organizational settings as well and should be tested in the organizational context in future works. Psychological ownership has demonstrated a significant effect on individuals' performance of security behaviors in situations where the data may not legally belong to the individual [4]. Despite an employee's lack of legal ownership over organizational data, the employee may still perceive a strong degree of psychological ownership over organizational data. In these cases, an employee will feel as protective of organizational data as his or her own personal data. The emotional connection (i.e., relatedness) an employee may perceive toward such data indicates that intrinsic motivation has the potential to be a powerful factor in organizational behaviors related to InfoSec, even though the data housed within the organization may not be, at face value, personally identifiable or seemingly relevant to the employee. We did not measure psychological ownership due to our focus on home users, but psychological ownership should be measured as a control in organizational settings to account for employees who may not be as deeply engaged as other employees are with their organization's data.

Conclusion

Home computer users are continuously presented with numerous threats to the security of their information. While effective solutions are often accessible, end users' motivation to perform secure behaviors may vary. An end user is far less likely to perform such behaviors if an adequate level of motivation is not present. Prior adaptations of PMT in InfoSec research have purported to motivate users toward the performance of secure behaviors through fear appeals. Our study highlights an important issue with prior InfoSec adaptations of PMT: because information is external to end users, the motivation to protect information may or may not be internalized by end users, allowing an end user's self-determination to play a role in predicting future behavior. Understanding end users' motivation to perform secure behaviors will lead to practices driving greater adoption of secure countermeasures and will contribute to an overall safer computing environment.

Our study offers a comparison of PMT, as previously adapted to InfoSec applications with fear appeals, to a novel adaptation of SDT with the formulation of self-determined appeals. The development of an alternate form of security appeals, which incorporates language that reinforces end users' autonomy, competence, and relatedness, leads to a greater intrinsic desire to protect information and an increased intention to perform a recommended countermeasure. Additionally, a motivational model based on SDT, rather than on PMT, explains more variance in intention while doing so more parsimoniously. While an appeal for adopting secure countermeasures will always, at least implicitly, originate from a particular threat, the prior focus on motivating behavior using fear may not be the most effective means of eliciting secure behaviors related to the protection of information. By recognizing end users' varying degrees of internalized motivation, our study presents an interesting and novel avenue for future works in behavioral InfoSec research.

Supplemental File

Supplemental data for the article can be found on the publisher's website at 10.1080/07421222.2017.1394083

References

1. Ajzen, I., and Fishbein, M. *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs, NJ: Prentice Hall, 1980.

2. Alkaldi, N., and Renaud, K. Why do people adopt, or reject, smartphone password managers? *1st European Workshop on Usable Security*. Darmstadt, Germany, 2016, pp. 1–14.

3. Alshammari, N.O.; Mylonas, A.; Sedky, M.; Champion, J.; and Bauer, C. Exploring the adoption of physical security controls in smartphones. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Los Angeles, CA: 2015, pp. 287–298.

4. Anderson, C.L., and Agarwal, R. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*, 3 (2010), 613–643.

5. Barki, H.; Paré, G.; and Sicotte, C. Linking IT implementation and acceptance via the construct of psychological ownership of information technology. *Journal of Information Technology*, *23*, 4 (October 2008), 269–280.

6. Baumeister, R.F., and Leary, M.R. The need to belong: Desire for interpersonal attachments as a fundamental human motivation. *Psychological Bulletin*, *117*, 3 (May 1995), 497–529.

7. Bhattacherjee, A. *Social Science Research: Principles, Methods, and Practices*. Tampa, FL: Open Access Textbooks, 2012.

8. Boss, S.R.; Galletta, D.F.; Lowry, P.B.; Moody, G.D.; and Polak, P. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*, 4 (2015), 837–864.

9. Bott, E. Two enterprise-worthy password managers: LastPass and RoboForm. *Tech Pro Research*, 2014. Available at www.techproresearch.com/article/two-enterprise-worthy-password-managers-lastpass-and-roboform/ (accessed on March 15, 2017)

10. Bulgurcu, B.; Cavusoglu, H.; and Benbasat, I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*, 3 (2010), 523–548.

11. Burnkrant, R.E., and Unnava, H.R. Self-referencing a strategy for increasing processing of message content. *Personality and Social Psychology Bulletin*, *15*, 4 (1989), 628–638.

12. Chatterjee, S.; Sarker, S.; and Valacich, J.S. The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*, 4 (2015), 49–87.

13. Crossler, R.E. Protection motivation theory: Understanding determinants to backing up personal data. In *43rd Hawaii International Conference on System Sciences*. Honolulu, HI: IEEE, 2010, pp. 1–10.

14. Crossler, R.E., and Bélanger, F. Determinants of individual security behaviors. In *Proceedings of the 2010 International Federation of Information Processing (IFIP) 8.11/11.13 Dewald Roode Workshop on Information Systems Security Research*. Waltham, MA, 2010, pp. 78–127.

15. Crossler, R.E., and Bélanger, F. An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *The Data Base for Advances in Information Systems*, *45*, 4 (2014), 51–71.

16. Crossler, R.E.; Bélanger, F.; and Ormond, D. The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, (2017). doi: https://doi.org/10.1007/s10796-017-9755-1

17. Crossler, R.E.; Johnston, A.C.; Lowry, P.B.; Hu, Q.; Warkentin, M.; and Baskerville, R. Future directions for behavioral information security research. *Computers and Security*, *32*, 1 (2013), 90–101.

18. D'Arcy, J.; Hovav, A.; and Galletta, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*, 1 (June 2009), 79–98.

19. Das, A., and Khan, H.U. Security behaviors of smartphone users. *Information and Computer Security*, *24*, 1 (2016), 116–134.

20. Davis, F.D.; Bagozzi, R.P.; and Warshaw, P.R. User Acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*, 8 (August 1989), 982–1003.

21. Davis, F.D.; Bagozzi, R.P.; and Warshaw, P.R. Extrinsic and intrinsic motivation to use computers in the workplace. *Journal of Applied Social Psychology*, *22*, 12 (1992), 1111–1132.

22. Deci, E.L., and Ryan, R.M. The empirical exploration of intrinsic motivational processes. In L. Berkowitz (ed.), *Advances in Experimental Social Psychology*. New York, NY: Academic Press, 1980, pp. 39–80.

23. Deci, E.L., and Ryan, R.M. The support of autonomy and the control of behavior. *Journal of Personality and Social Psychology*, *53*, 6 (December 1987), 1024–1037.

24. Faul, F.; Erdfelder, E.; Lang, A.G.; and Buchner, A. G *Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*, 2 (2007), 175–191.

25. Floyd, D.L.; Prentice-Dunn, S.; and Rogers, R.W. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*, 2 (November 2000), 407–429.

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

27. Gefen, D., and Straub, D.W. A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*, (2005), 91–109.

28. Gregor, S. The nature of theory in information systems. *MIS Quarterly*, *30*, 3 (2006), 611–642.

29. Gregor, S., and Klein, G. Eight obstacles to overcome in the theory testing genre. *Journal of the Association for Information Systems*, *15*, 11 (2014), i–xix.

30. Hair, J.F.; Hult, G.T.M.; Ringle, C.; and Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Thousand Oaks, CA: Sage, 2016.

31. van der Heijden, H. User acceptance of hedonic information systems. *MIS Quarterly*, *28*, 4 (2004), 695–704.

32. Herath, T., and Rao, H.R. Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*, 2 (April 2009), 106–125.

33. Ifinedo, P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*, 1 (November 2012), 83–95.

34. Jensen, M.L.; Dinger, M.; Wright, R.T.; and Thatcher, J.B. Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*, 2 (2017), 597–626.

35. Johnston, A.C., and Warkentin, M. Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*, 3 (2010), 549–566.

36. Johnston, A.C.; Warkentin, M.; and Siponen, M. An enhanced fear appeal framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*, 1 (2015), 113–134.

37. Komanduri, S.; Shay, R.; Kelley, P.G. et al. Of passwords and people: Measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Vancouver, Canada: ACM, 2011, pp. 2595–2604.

38. Lee, Y., and Larsen, K.R. Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*, 2 (March 2009), 177–187.

39. Lee, Y.; Lee, J.; and Hwang, Y. Relating motivation to information and communication technology acceptance: Self-determination theory perspective. *Computers in Human Behavior*, *51*, (2015), 418–428.

40. Liang, H.; Peng, Z.; Xue, Y.; Guo, X.; and Wang, N. Employees' exploration of complex systems: An integrative view. *Journal of Management Information Systems*, *32*, 1 (2015), 322–357.

41. Matteson, S. *Cybersecurity in an IoT and Mobile World: Defenses, Response Plans, and Greatest Concerns*. Louisville, KY: Tech Pro Research, 2016.

42. Menard, P.; Gatlin, R.; and Warkentin, M. Threat protection and convenience: Antecedents of cloud-based data backup. *Journal of Computer Information Systems*, *55*, 1 (2014), 83–91.

43. Miserandino, M. Children who do well in school: Individual differences in perceived competence and autonomy in above-average children. *Journal of Educational Psychology*, *88*, 2 (1996), 203–214.

44. Monroe, K.B. Buyers' subjective perceptions of price. *Journal of Marketing Research*, *10*, 1 (1973), 70–80.

45. Motulsky, H.J., and Ransnas, L.A. Fitting curvees to data using nonlinear regression: A practical and nonmathematical review. *FASEB Journal*, *1*, 5 (1987), 365–374.

46. Mylonas, A.; Kastania, A.; and Gritzalis, D. Delegate the smartphone user? Security awareness in smartphone platforms. *Computers and Security, 34*, (May 2013), 47–66.

47. Padayachee, K. Taxonomy of compliant information security behavior. *Computers and Security*, *31*, 5 (2012), 673–680.

48. Pahnila, S.; Siponen, M.; and Mahmood, A. Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Hawaii International Conference on System Sciences*. Waikoloa, HI, 2007, pp. 1–10.

49. Paternoster, R., and Simpson, S. Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Journal of Law and Society Association*, *30*, 3 (2009), 549–583.

50. Ponemon Institute. 2015 Cost of data breach study: United States. *Ponemon Institute Research Report* (2015), 1–22.

51. Posey, C.; Roberts, T.; and Lowry, P.B. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*, 4 (2015), 179–214.

52. Reis, H.T.; Sheldon, K.M.; Gable, S.L.; Roscoe, J.; and Ryan, R.M. Daily well-being: The role of autonomy, competence, and relatedness. *Personality and Social Psychology Bulletin*, *26*, 4 (2000), 419–435.

53. Ringle, C.M.; Wende, S.; and Will, A. SmartPLS. 2005. www.smartpls.de.

54. Rogers, R.W. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*, 1 (1975), 93–114.

55. Rogers, R.W. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protected motivation. In J.T. Cacioppo and R.E. Petty (eds.), *Social Psychophysiology: A Sourcebook*. New York, NY: Guilford Press, 1983, pp. 153–176.

56. Ryan, R.M. The nature of the self in autonomy and relatedness. In *The Self: Interdisciplinary Approaches*. New York, NY: Springer, 1991, pp. 208–238.

57. Ryan, R.M., and Deci, E.L. Intrinsic and extrinsic motivations: Classic definitions and new directions. *Contemporary Educational Psychology*, *25*, 1 (January 2000), 54–67.

58. Ryan, R.M., and Deci, E.L. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, *55*, 1 (January 2000), 68–78.

59. Thaler, R. Mental accounting and consumer choice. *Marketing Science*, *4*, 3 (1985), 199–214.

60. Thomson, M. Human brands: Investigating antecedents to consumers' strong attachments to celebrities. *Journal of Marketing*, *70*, 3 (2006), 104–119.

61. Vallerand, R.J. Toward a hierarchical model of intrinsic and extrinsic motivation. *Advances in Experimental Social Psychology, 29* (1997), 271–360.

62. Vallerand, R.J. Deci and Ryan's self-determination theory: A view from the hierarchical model of intrinsic and extrinsic motivation. *Psychological Inquiry*, *11*, 4 (2000), 312–318.

63. Vallerand, R.J.; Fortier, M.S.; and Guay, F. 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 (May 1997), 1161–1176.

64. Vance, A.; Lowry, P.B.; and Eggett, D. Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*, 4 (2013), 263–289.

65. Varma, S., and Marler, J.H. The dual nature of prior computer experience: More is not necessarily better for technology acceptance. *Computers in Human Behavior*, *29*, 4 (2013), 1475–1482.

66. Venkatesh, V. Creation of favorable user perceptions: Exploring the role of intrinsic motivation. *MIS Quarterly*, *23*, 2 (1999), 239–260.

67. Venkatesh, V. Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research*, *11*, 4 (2000), 342–365.

68. Venkatesh, V., and Davis, F.D. A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*, 2 (2000), 186–204.

69. Venkatesh, V.; Morris, M.G.; Davis, G.B.; Davis, F.D.; and Hall, M. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*, 3 (2003), 425–478.

70. Venkatesh, V.; Thong, J.Y.L.; and Xu, X. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*, 1 (2012), 157–178.

71. Villatte, N. *2015 Data Breach Investigations Report*. Basking Ridge, NJ: Verizon Enterprise Solutions, 2015.

72. Wall, J.D., and Palvia, P. Control-related motivations and information security policy compliance: The effect of reflective and reactive autonomy. In *AMCIS 2013 Proceedings*. Chicago, IL, 2013, pp. 1–9.

73. Wall, J.D.; Palvia, P.; and D'Arcy, J. A review and typology of security-related corruption controls: Setting an agenda for studying the behavioral effects of security countermeasures. In *Proceedings of the 2013 International Federation of Information Processing (IFIP) 8.11/11.13 Dewald Roode Workshop on Information Systems Security Research*. Buffalo, NY, 2013, pp. 1–35.

74. Winer, R.S. A reference price model of brand choice for frequently purchased products. *Journal of Consumer Research*, *13*, 2 (1986), 250–256.

75. Woon, I.M.Y.; Tan, G.W.; and Low, R.T. A protection motivation theory approach to home wireless security. In *International Conference on Information Systems*. Las Vegas, NV, 2005, pp. 367–380.

76. Workman, M. A test of interventions for security threats from social engineering. *Information Management and Computer Security*, *16*, 5 (2008), 463–483.

77. Workman, M.; Bommer, W.H.; and Straub, D.W. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*, 6 (September 2008), 2799–2816.

78. Wright, R.T.; Jensen, M.L.; Thatcher, J.B.; Dinger, M.; and Marett, K. Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research*, *25*, 2 (2014), 385–400.

79. Zeithaml, V.A. Consumer perceptions of price, quality, and value: A means-end model and synthesis of evidence. *Journal of Marketing*, *52*, 3 (1988), 2–22.

80. Zhao, L.; Detlor, B.; and Connelly, C.E. Sharing knowledge in social Q&A sites: The unintended consequences of extrinsic motivation. *Journal of Management Information Systems*, *33*, 1 (2016), 70–100.