Communications of the Association for Information Systems

Volume 45 Article 22

11-2019

Integrating Construal-level Theory in Designing Fear Appeals in IS Security Research

Davide C. Orazi
Monash University, davide.orazi@monash.edu

Merrill Warkentin
Mississippi State University

Allen C. Johnston
University of Alabama

Recommended Citation

Orazi, D. C., Warkentin, M., & Johnston, A. C. (2019). Integrating Construal-level Theory in Designing Fear Appeals in IS Security Research. Communications of the Association for Information Systems, 45, pp-pp. https://doi.org/10.17705/1CAIS.04522

Communications of the
Association for Information Systems

Research Paper DOI: 10.17705/1CAIS.04522 ISSN: 1529-3181

Integrating Construal-level Theory in Designing Fear Appeals in IS Security Research

Davide C. Orazi
Department of Marketing
Monash University, Australia
davide.orazi@monash.edu

Merrill Warkentin
Department of Management and Information Systems
Mississippi State University, USA

Allen C. Johnston
Department of Information Systems, Statistics, & Management Science
University of Alabama, USA

Abstract:

Organizations increasingly use fear appeals to motivate users to engage in behaviors that protect information security. Though academic interest in the topic has burgeoned, prior research has mainly focused on providing process evidence on how low- and high-threat security messages influence protective behaviors. According to protection motivation theory, however, the threat-appraisal phase, in which the receiver evaluates whether a fear appeal is threatening or not, follows exposure to the fear appeal. One can indeed design fear appeals to manipulate different dimensions, including the threat depicted and the coping response provided. These dimensions, in turn, influence protection motivation. The general focus on low- and high-threat messages runs the risks of 1) foregoing key theoretical insights that can stem from specific message manipulations and 2) inadvertently introducing message confounds. To address this issue, we introduce construal-level theory as the theoretical lens to design and identify potential confounds in fear-appeal manipulations. We further discuss how researchers can seamlessly integrate construal-level theory into information security studies based on protection motivation theory. Our work has important theoretical and methodological implications for IS security researchers.

Keywords: Information Security, Fear Appeals, Protection Motivation Theory, Construal-level Theory, Manipulation Confounds.

This manuscript underwent editorial review. It was received 03/28/2018 and was with the authors for 10 months for 2 revisions. Alvin Leung served as Associate Editor.

1 Introduction

As systems have become increasingly interconnected and digital technology has evolved at an exponential pace, we have witnessed an increasing number of security breaches, data thefts, and privacy violations in sectors as diverse as healthcare, manufacturing, and financial services (Cisco, 2017). Information security breaches hit businesses of all sizes and have proven to have substantial market effects (Wang, Kannan, & Ulmer, 2013). For example, the Ponemon Institute (2017) institute has estimated such breaches to cost U.S. large businesses US$7.35 million on average. While the U.S. Government has called for strategies to counter attacks from hackers (Cisco, 2017), employees still remain the weakest link in the information security chain (Ernst & Young, 2017) due to intentional leaks (Kaspersky Lab, 2017) and carelessness about security policies (Sharp, 2017). Therefore, understanding how to persuade employees to adopt protective behaviors has increasing relevance in information security research (Johnston & Warkentin, 2010; Johnston, Warkentin, & Siponen, 2015).

To prevent employees from violating information security policies, CIOs and information security managers now often embed fear appeals in messages to stimulate protective behaviors against threats that come from external entities and organizational insiders (Boss, Galletta, Lowry, Moody, & Polok, 2015). Fear appeals are persuasive messages that focus on motivating individuals to adhere to protective recommendations to prevent impending threats (Keller & Lehmann, 2008). Given the managerial relevance of identifying and mitigating threats to information systems (IS) security (Willison & Warkentin, 2013), research on the effect that fear appeals have on compliance with security policies has burgeoned (Johnston & Warkentin, 2010; Anderson & Agarwal, 2010; Boss et al., 2015; Johnston et al., 2015; Wall & Buche, 2017; Wang, Li, & Rao, 2017; Moody, Siponen, & Pahnila, 2018; Johnston, Warkentin, Dennis, & Siponen, 2019).

As the discipline advances and information security fear-appeal research gains momentum and sophistication, scholars have devoted substantial efforts to understanding what drives compliance with information security recommendations (Lee & Larsen, 2009; Johnston & Warkentin, 2010; Moody, Siponen, & Pahnila, 2018). Protection motivation theory (PMT) (Rogers, 1975; Maddux & Rogers, 1983) has been the dominant paradigm in information security for predicting whether individuals will adopt protective behaviors. The theory has seen widespread use because, among other reasons, it allows researchers to clearly disaggregate the threat and the efficacy elements in a fear appeal and, thus, to to study how different elements that capture threat appraisals (e.g., severity and susceptibility) and coping appraisals (e.g., response efficacy and self-efficacy) influence compliance motivation (Maddux & Rogers, 1983). Thus, most recent research efforts in information security have focused on assessing the nomological and predictive validity of alternative models based on PMT (Johnston & Warkentin, 2010; Orazi & Pizzetti, 2015; Boss et al., 2015; Johnston et al., 2015). This laudable endeavor evokes the earliest days of the technology adoption model (TAM) when researchers performed several studies to assess its parsimony, generalizability, and predictive power in comparison to its originator, the theory of reasoned action (Lee, Kozar, & Larsen, 2003). Testing new models to advance or challenge the nomological and predictive validity of established ones signifies an active research domain and the normal flow of theorizing in and across paradigmatic disciplines.

Despite substantial advances, in comprehensively reviewing experimental designs and fear-appeal manipulations in information security research, Boss et al. (2015) found that most information security research that has used fear appeals has favored surveys (e.g., Herath & Rao, 2009; Lee & Larsen, 2009) over experimental designs, which has limited novel insights based on causal evidence from emerging. Even when studies have used experimental designs, they have typically manipulated general levels of low and high threat (Boss et al., 2015). Manipulating general threat levels rather than specific fear appeal elements (e.g., nature of the negative consequences for noncompliance, message framing, etc.) conflicts with protection motivation theory, which posits that threat appraisal influences exposure to a fear appeal (Rogers, 1975; Maddux & Rogers, 1983; Wall & Buche, 2017). Information security researchers should manipulate specific fear appeal dimensions (i.e., the message) and then measure their effects on threat appraisal (i.e., the process through which the message receiver assesses the severity and susceptibility to the impending threat). Thus, by using general low and high threat manipulations, researchers have focused attention on the process through which protection motivation unfolds to the point we know a great deal about *how* fear appeals produce their persuasive effects but not *which* fear appeals produce the strongest effects. In turn, this approach limits researchers from generating novel theoretical insights from studying specific, theory-driven dimensions of fear-appeal manipulations. It also diminishes researchers' exposure to experimental research, which increases the risk that they will inadvertently introduce confound effects when designing manipulations. (e.g., Boss et al. 2015).

In order to shift the current research paradigm to encompass a more nuanced focus on fear-appeal manipulations, we provide an actionable framework to design fear-appeal manipulations in information security research and identify confound effects in current experimental work. To this end, we draw on the construal-level theory of psychological distance (Trope, Liberman, & Wakslak, 2007; Trope & Liberman, 2010), a flexible theoretical framework that researchers have successfully employed in psychological and marketing research to manipulate message dimensions, which includes the nature of behavioral consequences (Orazi, Lei, & Bove, 2015), the temporal unfolding of negative consequences (Murdock & Rajagopal, 2017), the framing of coping responses in terms of *how* versus *why* (White, MacDonnell, & Dahl, 2011), and so on. Construal-level theory has also demonstrated compatibility with prospect theory (see White et al., 2011; Orai et al., 2015), which makes it particularly suitable for manipulating fear appeals that deal with loss and gain frames.

This paper proceeds as follows: in Section 2, we provide the theoretical background on information security fear-appeal research and the dominant paradigm we employ in this paper: protection motivation theory. In Section 3, we introduce construal-level theory as a relevant theoretical lens to design fear appeals. We provide an illustrative example of its application using existing information security research. We also explain why construal-level theory is compatible with protection motivation theory and offer testable propositions that can inform future research. Finally, in Section 4, we conclude the paper.

2 PMT in Information Security

Protection motivation theory (PMT) (Rogers, 1975; Maddux & Rogers, 1983) represents the dominant behavioral-change paradigm for explaining individuals' motivations to adopt desirable information security behaviors (Lee, Larose, & Rifon, 2008; Lee & Larsen, 2009; Johnston & Warkentin, 2010; Orazi & Pizzetti, 2015; Boss et al., 2015; Johnston et al., 2015; Johnston et al., 2019). PMT predicts that an individual's intention to adhere to a prescribed recommendation on how to prevent a potential threat depends on four core variables: 1) threat severity, 2) threat susceptibility, 3) coping response efficacy, and 4) self-efficacy (Floyd, Prentice-Dunn, & Rogers, 2000). Perceived threat severity refers to individuals' estimation or beliefs about the threat's seriousness (*severity*). Perceived threat susceptibility refers to individuals' estimation about how likely they will be to personally experience the threat (*susceptibility*). Response efficacy refers to the degree to which individuals believe the response will effectively alleviate or eliminate the stated threat (*response efficacy*). Self-efficacy refers to the degree to which individuals believe in their own ability to enact the recommended response (*self-efficacy*). According to PMT, individuals will most likely adhere to the recommended response when they perceive a threat as severe and as likely to personally affect them and when they perceive the proposed recommendation as an effective and viable solution for coping with it (Witte & Allen, 2000).

Since the theory emerged, researchers have enriched it with 1) fear arousals, 2) rewards for non-adherence, and 3) costs for adherence ("response costs" in terms of time or inconvenience). Witte (1994) included fear arousal in the theory to capture affective reactions to highly threatening messages. According to Witte, highly threatening messages coupled with perceptions of low efficacy evoke fear, which prompts individuals to focus on controlling their fear rather than coping with the threat. Other researchers included rewards for non-adherence and costs for engaging in the recommended response in the theory to consider behavioral economic theory applied to self-regulation. Accordingly, high non-adherence rewards reduce a threat's perceived magnitude (i.e., severity and susceptibility), whereas high adherence costs reduce the coping response's overall appeal (Floyd et al., 2000). Several meta-analyses have confirmed significant relationships between the PMT variables and intentions to adopt the recommended response (Milne, Sheeran, & Orbell, 2000; Witte & Allen, 2000; de Hoog, Stroebe, & de Wit, 2007).

In information security research, scholars have applied PMT as both a behavioral response theory to explain a response to a fear appeal stimulus (Johnston & Warkentin, 2010; Johnston et al., 2015, 2019) and as a theory to understand threat response intentions in more static environments (Herath & Rao, 2009; Lee & Larson, 2009). Warkentin (2010) and Boss et al. (2015) have both made notable contributions in improving PMT's predictive and nomological validity in information security research while testing the effect of fear-appeal manipulations. First, Johnston and Warkentin (2010) reconciled issues about threat severity's and susceptibility's seemingly weak direct effects on intention by reconceptualizing

PMT as a multiple mediation model called the fear appeal model (FAM) in which response efficacy and self-efficacy mediate such effects. Researchers in both the IS (Johnston et al., 2015, 2019) and marketing (Orazi & Pizzetti, 2015) disciplines have successfully replicated the FAM using different populations, contexts, and estimation methods. Second, Boss et al. (2015) extended PMT's nomology particularly by re-introducing fear arousal as an affective mediator of protection motivation and by demonstrating how different fear-appeal manipulations in information security (i.e., low vs. high threat) have differential effects on perceptions of threat severity, threat susceptibility, coping efficacy, and self-efficacy.

While the discourse around testing different predictive models has much importance for progressing information security research as a discipline, one key concern emerges from Boss et al.'s (2015) recent work in which they review PMT-based information security research. The authors lament the overreliance on survey designs that measure users' compliance intentions with information security policies (e.g., Lee et al., 2008; Herath & Rao, 2009; Lee & Larsen, 2009). Information security fear-appeal researchers who study the motivation to adopt protective behaviors typically focus on either measuring the baseline level of compliance with information security recommendations (Lee et al., 2008; Lee & Larsen, 2009) or testing to what extent exposure to an information security fear-appeal manipulation increases the degree to which users accept recommended security actions (e.g., Johnston & Warkentin, 2010; Boss et al., 2015).

Researchers commonly specify predictive models based on guidance from the PMT and information security literatures and then gather data to support or disconfirm the hypotheses (e.g., Lee et al., 2008; Lee & Larsen, 2009; Johnston & Warkentin, 2010; Boss et al. 2015). When researchers use a model to measure user baseline intentions to engage in recommended responses to threats contained in persuasive messages, they do not need fear-appeal manipulations. In such cases, researchers typically design survey instruments to collect data from items that reflect users' perceptions. These scales typically measure users' perceptions about a threat's severity and their susceptibility to it, their perceptions about whether the coping response will effectively prevent or alleviate the threat, their beliefs about whether they can implement the coping response, and their motivation to adopt protective actions (e.g., Lee et al., 2008; Lee & Larsen, 2009). They then test data against the specified model to verify the hypotheses.

At times, however, researchers may want to compare two or more fear appeal conditions to determine their effectiveness depending on the information security context (Crossler et al., 2013). To this end, researchers will use experimental designs and manipulate one or more message components or various message dimensions to explore how variations in one dimension influences how users perceive PMT variables and the ensuing protection motivation. Boss et al. (2015), however, note that few studies actually incorporate fear-appeal manipulations in their design (Johnston & Warkentin, 2010; Crossler et al., 2013; Johnston et al., 2015; Boss et al., 2015) even though PMT theoretically assumes that one will use them and they represent a practical way to instill protection motivation in users. Moreover, most such studies employ general low and high threat manipulations. This approach limits our understanding about the effectiveness of fear appeals. Manipulating threat levels (low vs. high) rather than specific dimensions of the fear appeal foregoes the rich insights that could emerge from integrating different theoretical frameworks that connect to each element in the fear-appeal manipulation. For instance, the fear appeal can manipulate the nature of the behavioral consequences stemming from misbehavior (Orazi, Lei, & Bove, 2015), the timeframe through which behavioral consequences unfold (Murdock & Rajagopal, 2017), or their social focus in terms of their detrimental effects on users and/or organizations (Warkentin, Walden, Johnston, & Straub, 2016). In turn, each manipulated dimension contributes to how users appraise threat overall when exposed to a fear appeal. Failure to distinguish the complex layers that constitute a fear appeal increases the risk that one manipulates multiple design elements with different effects on protection motivation at once. In turn, one cannot determine which element in the fear-appeal manipulation causes a variation in the observed dependent variables (e.g., protection motivation).

3 A Construal-level Taxonomy for the Design of Fear Appeals

Fear-appeal manipulations play a key role in IS research, and their development and validation requires the utmost attention. Because most fear-appeal research outside the IS discipline rests on experimental designs, several scholars who study how one should communicate threats and remedies advocate a reductionist approach to fear-appeal manipulations: to reduce messages to their structural components to allow one to meaningfully compare their effects (LaTour & Rotfeld, 1997; Shehryar & Hunt, 2005; Orazi et al., 2015).

However, thus far, the literature has offered little guidance in terms of a theory-driven reference framework to help researchers design fear appeals. The obvious reason for this shortcoming is that typical information security fear appeals comprise multiple visual and textual elements, and no single theory can encompass the plethora of potentially manipulable variables. We agree with such an assessment, but, at the same time, recognize that only by isolating and studying the individual and interactive effects of each structural component of a fear appeal can we understand when, why, and how a message produces the intended effects. Explaining the multi-faceted nature of fear-appeal manipulations requires broadly applicable theories. We believe construal-level theory (Trope et al., 2007; Trope & Liberman, 2010) to represents one such theoretical framework.

3.1 Construal-level Theory and Types of Psychological Distance

Construal-level theory (CLT) rests on the core tenet that people have direct experience only of the here and now and create mental simulations that they abstract from this experience (namely, construals) to represent objects and events that they cannot directly access through their senses (Fujita, Trope, Liberman, & Levin-Sagi, 2006; Eyal, Liberman, & Trope, 2008; Trope & Liberman, 2010). The abstractness of these construals depends on their psychological distance from the self; namely, the subjective perception that something “takes place further into the future, …occurs in a more remote location, …happens to people less and less like oneself, and …is less likely to occur” (Trope et al., 2007, p. 84). Thus, mental construal depends on information availability since the more people move away from directly experiencing objects and events, the less available information they have about said object and events.

Because the way in which individuals represent psychological objects depends on the information available to them, representing remote things requires more abstract construals than representing close things (Nussbaum, Trope, & Liberman, 2003). In other words, individuals construe psychologically distant objects in general and abstract terms (i.e., high construal) by focusing on essential features and considering the superordinate or “why” level. Conversely, individuals construe psychologically close objects in specific and concrete terms (i.e., low construal) by focusing on incidental features and considering the subordinate or “how” level (Fujita et al., 2006; Trope & Liberman, 2010).

Psychological distance, however, is a multi-faceted construct that researchers have divided into at least four typologies: 1) temporal, 2) spatial, 3) social, and 4) hypothetical (Bar-Anan, Liberman, & Trope, 2006; Trope & Liberman, 2010). All types of psychological distances relate to each other and share the same reference point in the individual’s experience and familiarity with a target object or event (Bar-Anan et al., 2006).

Temporal distance refers to individuals’ perception that an event occurs at a time near (proximal) versus far (distal) from them (e.g., the near vs. distant past or future). The longer the temporal distance, the higher the construal level individuals use to mentally represent the object or event. Converging evidence demonstrates that individuals construe events located in the distant (vs. close) past or future with more abstract (vs. concrete) features (Liberman, Sagristano, & Trope, 2002; Wakslak, Trope, Liberman, & Alony 2006; Trope & Liberman, 2010).

Spatial distance refers to individuals’ perception that an object or event occurs in a place near versus far from them. Smith and Trope (2006) effectively capture the relationship between the spatial distance and construal level in their example about a forest and trees: from a high spatial distance, people see a forest, but, from a low spatial distance, they see the trees. Similarly to temporal distance, empirical evidence demonstrates that individuals construe distant (vs. close) places in more abstract (vs. concrete) terms (Fujita et al., 2006).

Social distance refers to the extent to which an individual perceives others to be different and unfamiliar, which includes differences in terms of group belonging and status (Bar-Anan et al., 2006). The higher the social distance, the higher the construal level such that individuals describe dissimilar people (Nussbaum et al., 2003), people who belong to social circles that individuals do not identify with (Liberman, Trope, & Wakslak, 2007), and people in positions of high power (Popper, 2013) in more abstract terms. In addition, people tend to describe their own behavior in terms of situational and concrete factors that operate in the moment of action, whereas they describe others’ behaviors in dispositional and abstract terms (Trope & Liberman, 2010).

Hypothetical distance refers both to the perceived likelihood that the construed event will occur and to the extent to which the construed event reflects reality (Bar-Anan et al., 2006). The less an event will likely occur or the more detached from reality an object or event, the higher the construal level required. Research demonstrates that people who imagine unlikely events describe them in more abstract terms and focus on their core and essential features (Wakslak, Trope, Liberman, & Alony, 2006).

We contend that psychological distance and its multiple facets pertain to information security research for two key reasons. First, the fact that multiple types of psychological distance exist allows one to manipulate different fear appeal dimensions using the same overarching theoretical framework. Second, researchers have mapped psychological distance's various effects that and, thus, provided guidelines on the likely effects that embedding low and high construals in a fear appeal will produce. We return on this latter point in Section 3.3 when we provide testable propositions. For now, we explain the relevance of construal-level theory for designing information security fear appeals and provide illustrative examples based on prior information security research.

3.2 Explaining Information Security Fear Appeals through Construal-level Theory

Fear appeals typically manipulate two elements: 1) an impending threat that will potentially cause negative consequences and 2) a coping response whose implementation minimizes the risk that the threat will occur (Keller & Lehmann, 2008). However, when designing a fear appeal's threat component, one has to consider more than the consequences' magnitude. Prior research that has used construal-level theory as a lens to categorize persuasive messages' different components has provided support for operationalizing both their threat (Orazi et al., 2015; Murdock & Rajagopal, 2017) and coping components (Ülkümen & Cheema, 2011; White et al., 2011). Thus, one can explain the negative consequences and the coping response that a fear appeal depicts in terms of psychological distance. Imagine a fear appeal that depicts the threat of keylogging and identity theft for IS users that browse streaming websites on office desktops. The fear appeal may present the threat 1) as immediate or delayed in time (i.e., temporality), 2) as widespread and affecting the vast majority of users or as relatively infrequent (i.e., hypotheticality), and 3) as a threat for the user itself or for other users and the organization as a whole (i.e., social focus).

In this same example, the coping response that the fear appeal offers as a way to minimize the risk of negative consequences 1) may have immediate or delayed effectiveness in preventing the threat (i.e., temporality), 2) may have a higher or lower probability of success once implemented (i.e., hypotheticality), and (3) may provide prescriptive information on how to cope with the threat or ideological information on why one should cope with the threat (i.e., framing). Individuals can construe actions at a low level by focusing on *how* to perform them or at a high level by focusing on *why* they should perform an action or what value achieving it has (Freitas, Gollwitzer, & Trope, 2004; Liviatan, Trope, & Liberman, 2008).

Thus, construal-level theory pertains to information security research because it can help one articulate a framework to classify fear appeal components in terms of low versus high construal. Accordingly, such a framework can better explain the effects of these components, which can lead to improvements in their design and efficacy. Further, such a framework can help to reduce the risk that one inadvertently includes confounds in the fear-appeal manipulation. Subtle differences in the threat manipulation can lead to differences in the overall construal level and, thus, increase or decrease the absolute influence of the threat manipulation of protection motivation.

Consider the following example: Boss et al. (2015) recently compared different frameworks based on PMT to understand which one more effectively predicted whether users comply with information security fear appeals. Their fear-appeal manipulation differed in terms of low versus high threat by varying threat severity (harmless vs. catastrophic consequences) and threat susceptibility (low risk vs. high risk). This variation allowed them to compare how predictive models that rely on different endogenous variables explain user compliance across low- versus high-threat messages. In addition to threat severity and susceptibility, however, their fear-appeal manipulation also differed in terms of 1) the negative consequences' temporality and 2) the likelihood that the user would remove the detected virus (i.e., hypotheticality of the coping response).

With regard to temporality, the low-threat condition depicted harmless negative consequences, (i.e., "user name will be changed to "dumb user" after one month) that would happen after a full month (delayed temporality). In contrast, the high-threat condition depicted catastrophic negative consequences, (i.e., "Hard-drive will become unusable after next restart") that would occur after the next system restart (for the original stimuli, see Boss et al., 2015). Note that negative consequences' temporality (i.e., one month vs. next restart) differs from their severity (i.e., wiping a hard-drive vs. changing one's username), and this difference affects how users perceive the threat. According to Murdock and Rajagopal (2017), immediate threats more effectively stimulate protection motivation than delayed threats.

With regard to the likelihood that the user would remove the detected virus, the low-threat condition showed that the user had a 95 percent chance to successfully remove the virus. This high probability of success likely characterized the coping response as very effective. The high-threat condition showed that the user had only a five percent chance to successfully remove the virus, which likely characterized the coping response as ineffective. Yet, a threat's magnitude and the coping response's efficacy theoretically differ, which means one should clearly separate them in designing a fear appeal and typically hold the coping response constant across conditions. However, Boss et al. (2015) did not effectively isolate the treatment in their experimental design.

Table 1 explains how the abovementioned example differentially manipulates fear appeal dimensions in terms of construal levels across the two experimental conditions. In addition, the table presents selected research papers in the IS research domain that researchers may find useful to understand how they can manipulate fear appeal components in terms of construal level. Anderson and Agarwal (2010), for instance, manipulated self-view by focusing the negative consequences on either the individual user or all users of the Internet. Specifically, we can see that individuals perceive a focus on self as psychologically close to them and, thus, construe it more concretely (i.e., low construal) but perceive a focus on other as psychologically distant and, thus, construe it more abstractly (i.e., high construal). Johnston and Warkentin (2010), on the other hand, simply compared the effectiveness of a high-threat fear appeal against a control condition. In a message that urged users to protect themselves against phishing, they presented a concrete threat (i.e., low construal) described as likely to occur and targeting the user, while providing a concrete coping response (i.e., low construal) that explained how to implement an effective and timely coping response.

Table 1. Construal-level Comparison of Experimental Stimuli used in Selected Fear-appeal Research

Research references	Threat manipulation			Coping manipulation		
	Temporality of threat (1)	Hypotheticality of threat (2)	Social focus (3)	Temporality of coping (4)	Hypotheticality of coping (5)	Coping response frame (6)
Anderson & Agarwal (2010)	NA	Likely (LC)	Manipulated self (LC) vs. others (HC)	NA	NA	Both how and why
Johnston & Warkentin (2010)	NA	Likely (LC)	Self (LC)	Immediate (LC)	Likely (LC)	How (LC)
Jenkins, Grimes, Proudfoot, & Lowry (2014)	NA	Likely (LC)	Self (LC)	Immediate (LC)	Likely (LC)	How (LC)
Boss et al. (2015)	Confounded: High threat = immediate (LC); Low threat = Delayed (HC)	Likely (LC)	Self (LC)	Immediate (LC)	Confounded: High threat = 5% chance (HC); low threat = 95% chance (LC)	How (LC)

Note:
(1,4) Immediate = LC; delayed = HC.
(2,5) Likely = LC; unlikely = HC.
(3) Self = LC; others = HC.
(6) How = LC; why = HC.
NA = not applicable, LC = low construal, HC = high construal.

3.3 The Effects of Construal Level: Propositions for Information Security Researchers

The examples above demonstrate how designing fear appeals is a tricky process and how the presence of different variables in the same manipulation complicates one's ability to interpret causal effects. However, a reference framework, such as construal-level theory, can help one to more clearly understand how each manipulated dimension produces its effect on protection motivation and the mechanisms that underlie the process.

One can derive testable propositions on these effects based on prior research on construal level. For instance, converging evidence demonstrates that predictions about distant events tend to be more schematic and abstract than predictions about closer events (Gilbert & Wilson, 2007). In the fear-appeal context, we also know that negative consequences that individuals appraise as low construals (e.g., because they unfold earlier in time) more effectively stimulate behavioral change than negative consequences that individuals appraise as high construals (Murdock & Rajagopal, 2017). Future information security research should first map the construal level of different negative consequences and then manipulate specific aspects of a message's threat component (see Table 1). Based on existing research and the notion that, when thinking about an event, high-level construals lead individuals to focus on an event's causes whereas low-level construals lead individuals to focus on the effects (Rim, Trope, Liberman, & Shapira, 2013), we expect that low construal threat manipulations will increase protection motivation. Thus, we propose:

> **P1:** In a fear appeal, manipulating the a) temporality, b) hypotheticality, and c) social focus of the negative consequences as low construal (i.e., concrete) increases protection motivation.

We justify this effect based on the fact that low construal (concrete) threats increase threat severity and susceptibility in the threat-appraisal phase. Since concrete representations of negative outcomes tend to be more persuasive (Eyal et al., 2008) because they focus users' attention on the nefarious effects that the threat produces, low construal threats should increase threat severity. At the same time, CLT contends that individuals perceive low construals as psychologically closer to the self. Past research in marketing communications has found that negative consequences that are a) temporally close, b) likely to occur, and c) focused on the self increase perceived susceptibility to a threat (Murdock & Rajagopal, 2017). Users are more likely to perceive a cyber-security threat that evokes imminence and focuses on users rather than organizations as threatening, which contributes to heightened levels of threat appraisal. Thus, we propose:

> **P2:** The effect of low construal negative consequences is carried over protection motivation through a) increased threat severity and b) increased threat susceptibility.

Turning to a fear appeal's coping-response component, we have two differing expectations depending on the construal level. When it comes to the coping response's temporality and hypothetical effectiveness, we can reasonably believe that low construals will have a stronger effect on protection motivation. Providing a user with a coping response that does not take up much time and describes itself as proven to remove a threat will likely increase perceptions about the solution's efficiency (i.e., less time) and effectiveness (i.e., higher likelihood to succeed). Thus, we propose:

> **P3:** In a fear appeal, manipulating the a) temporality and b) hypotheticality of the coping response as low construal (i.e., concrete) increases protection motivation.

When it comes to the framing that the coping response adopts in terms of *how* (low construal) versus *why* (high construal) users should adopt protective recommendations, different effects may unfold. As we mention in Section 3.2, individuals can construe actions at a low level by focusing on *how* to perform them or at a high level by focusing on *why* they should perform an action or what value achieving it has (Freitas et al., 2004; Liviatan et al., 2008). The few studies in information security research that manipulate the coping response in their fear appeals (e.g., Johnston et al. 2015) have centered on feasibility and provided tips and actions on how to avoid negative consequences (i.e., low construal). We currently know nothing about users' reactions to fear appeals that focus on desirability and the reasons why one should comply with the recommended response (i.e., high construal). Yet, prior psychological research suggests that high-level construals facilitate self-control (Fujita, Trope, Liberman, & Levin-Sagi, 2006). As such, we have reason to believe that more inspirational coping responses (i.e., why) may exert a stronger influence on protection motivation. Thus, we propose:

> **P4:** In a fear appeal, manipulating a coping response's framing as high construal (i.e., abstract) increases protection motivation.

Based on the above arguments, we expect that increased coping response efficacy and self-efficacy will mediate the effects of the coping response manipulation. Supporting this prediction, Wall and Warkentin (forthcoming) found that fear appeals with stronger perceived argument quality increased efficacy levels. Timely and effective coping responses (i.e., concrete) are more likely to increase perceived coping response efficacy. At the same time, if a security response requires less time to be implemented and promises to eliminate the threat, users' self-efficacy will likely increase due to the provision of an effective coping response. Thus, we propose:

> **P5:** The effect of both low and high construal level coping responses is carried over protection motivation through a) increased coping response efficacy and b) increased self-efficacy.

As we discuss above, CLT's broad applicability as a design framework opens the possibility to manipulate multiple elements in the same fear appeal in terms of low versus high construal. In such occurrences, the different construal levels of the threat and coping components may interact. For instance, prior psychological research shows that psychological distance influences choice and that feasibility concerns (i.e., how can we achieve something) progressively lose importance to desirability concerns (i.e., an achievement's value) as psychological distance increases (Liviatan et al., 2008). If the same relationship holds for protective behaviors, then high-construal coping responses should be most effective when coupled with more distant temporal horizons. Both psychology and marketing research have documented this "construal-fit" effect (see Lee, Lee, & Kern, 2011; White et al., 2011). Tying back the construal level of the coping response to the consequences' construal level, the construal-fit effect that White et al. (2011) isolated proposes that the effectiveness of a message that prescribes behavioral compliance increases when its structural components have the same construal level. In our context, we expect matching the negative consequences' construal level to the coping response's construal level to enhance protection motivation by activating a fitting (vs. unfitting) construal mindset. Thus, we propose:

> **P6:** A fear appeal increases in effectiveness when the negative consequences and the coping response have matching construal levels.

As a final consideration, while some researchers may express concern that CLT and PMT constitute distinct theoretical frameworks and, thus, that one should test them in isolation, we believe that one can seamlessly integrate them. In line with the structuralist approach that we advocate here, researchers who investigate the effectiveness of communications must reduce messages to their fundamental components to to meaningfully compare their effects (LaTour & Rotfled, 1997; Shehryar & Hunt, 2005; Orazi, Lei, & Bove, 2015). The message and the receiver, however, constitute distinct elements in the communication process. *What* a fear appeal manipulates produces specific effects on protection motivation, but *how* this process unfolds depends on the way the user evaluates and interprets the fear appeal's different components (namely, the threat element and the coping response). This interpretative process results in what the PMT literature calls threat and coping appraisals (Rogers, 1975; Maddux & Rogers, 1983).

In this sense, one can use CLT or other theories to aptly manipulate both the threat component and the coping response that a fear appeal provides. On the other hand, one can use PMT to effectively describe the underlying mechanisms through which a fear appeal produces its effects. In summary, we believe that theory-driven manipulations, such as manipulations that CLT inform, can provide answers to *what* questions, whereas process frameworks such as PMT can provide answers to *how* questions. This distinction between message and receiver enables seamless theoretical integrations. To summarize, in Figure 1, we visualize the seamless integration between construal-level theory and protection motivation theory and locate our propositions at different levels in the manipulated fear appeal.

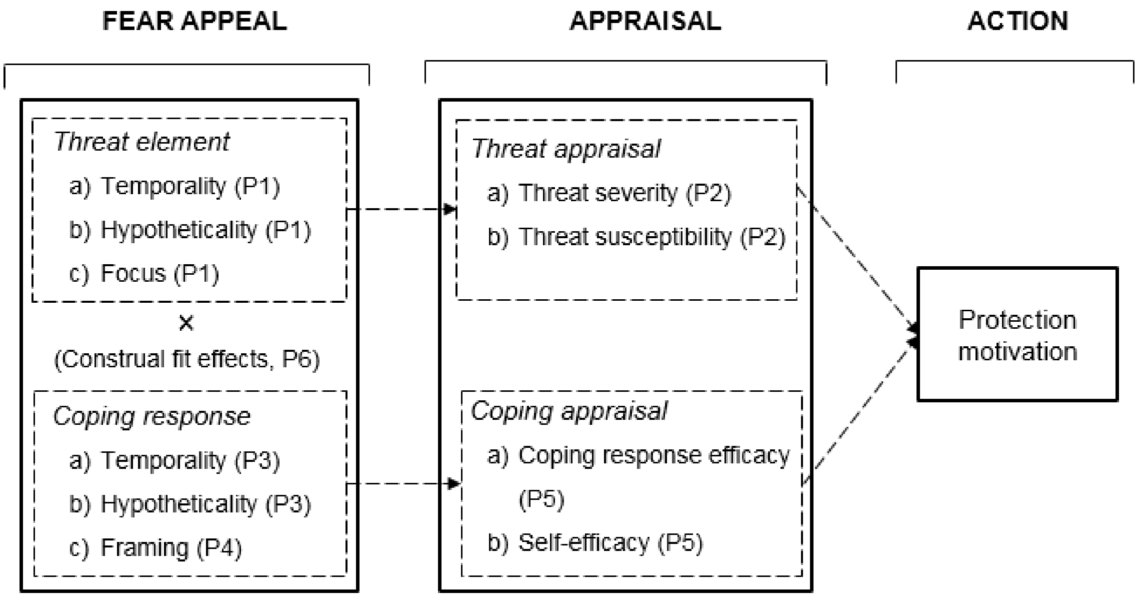

Figure 1. Compatibility between CLT (Message-level Manipulations) and PMT (Individual-level Appraisals)

4 Conclusion

Fear appeals have emerged as effective communication tools to promote and increase users' adherence to information security recommendations. Converging research based on the protection motivation theory has developed robust predictive frameworks to assess the effectiveness of such fear appeals in information security and related contexts (Johnston & Warkentin, 2010; Orazi & Pizzetti, 2015; Johnston et al., 2015, 2019). However, the current focus remains on process models that can explain the underlying mechanisms through which general (typically low vs. high threat) fear appeals produce their effects. As existing research focuses on answering research questions about *how* fear appeals produce their effects, we propose a theory-driven framework to extend the current focus on *which* fear appeals and, most importantly *why* fear appeals produce the strongest effects on protection motivation.

Focusing on designing theory-driven fear appeals represents the first step to embrace a paradigm shift in IS research. To this end, we present construal-level theory as a viable and broadly applicable theoretical lens. Classifying fear appeals' design elements through construal-level theory may afford new research directions in the information security discipline and, at the same time, stimulate experimental research based on designing rigorous and unconfounded fear appeals. IS research has a rich, positivist tradition in advancing scientific rigor by providing clear guidelines and calling for more efforts in validating IS research instruments (Straub, 1989; Straub, Boudreau, & Gefen, 2004; Venkatesh, Brown, & Bala, 2013; Steelman, Hammer, Limayem, 2014; Larsen & Bong, 2016), and we hope this paper contributes to this direction.

At the same time, we fully acknowledge that no single theory can explain all the facets of message design. With our work, we highlight the need for care when designing fear appeals to avoid unwanted confounds. One way to systematize how we design fear appeals involves moving away from manipulating low and high threat levels in general and focusing more on theory-driven design. While we use construal-level theory as a theoretical lens to explain previous confounded fear appeals and to develop testable propositions for future research, many other theoretical frameworks may inform how researchers design IS fear appeals. We also believe future research into fear appeal design can hone in on the sequential versus parallel nature of threat- and coping-appraisal processes. Previous research has presented appraisals processes as either sequential or parallel, but, in reality, these appraisal processes may be more hybrid in nature and depend highly on the context. We hope this paper encourages researchers to appreciate the necessity for rigorous, theory-driven fear appeal design.

References

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

Bar-Anan, Y., Liberman, N., & Trope, Y. (2006). The association between psychological distance and construal level: Evidence from an implicit association test. *Journal of Experimental Psychology: General, 135*(4)**,** 609-622.

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

Cisco. (2017). *Cybersecurity roadmap*. Retrieved from https://learningnetwork.cisco.com/community/it_careers/2017-cybersecurity-roadmap

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

de Hoog, N., Stroebe, W., and de Wit, J. B. (2007). The impact of vulnerability to and severity of a health risk on processing and acceptance of fear-arousing communications: A meta-analysis. *Review of General Psychology*, *11*(3), 258-285.

Ernst & Young. (2017). *The state of cyber resilience*. Retrieved from http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016

Eyal, T., Liberman, N., & Trope, Y. (2008). Judging near and distant virtue and vice. *Journal of Experimental Social Psychology*, *44*(4), 1204-1209.

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

Freitas, A. L., Gollwitzer, P., & Trope, Y. (2004). The influence of abstract and concrete mindsets on anticipating and guiding others' self-regulatory efforts. *Journal of Experimental Social Psychology*, *40*(6), 39-752.

Fujita, K., Trope, Y., Liberman, N., & Levin-Sagi, M. (2006). Construal levels and self-control. *Journal of Personality and Social Psychology*, *90*(3), 351-367.

Gilbert, D. T., & Wilson, T. D. (2007). Prospection: Experiencing the future. *Science*, *317*(5843), 1351-1354.

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

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, *20*(2), 196-213.

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

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

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*, *50*(2), 245-289.

Kaspersky Lab. (2017). *From the top: What executives need to know about cybersecurity*. Retrieved from https://it-securityworld.com/assets/whitepapers/Jan20180504.pdf

Keller, P. A., & Lehmann, D. R. (2008). Designing effective health communications: A meta-analysis. *Journal of Public Policy & Marketing*, *27*(2), 117-130.

Larsen, K. R., & Bong, C. H. (2016). A tool for addressing construct identity in literature reviews and meta-analyses. *MIS Quarterly*, *40*(3), 529-551.

LaTour, M. S., & Rotfeld, H. J. (1997). There are threats and (maybe) fear-caused arousal: Theory and confusions of appeals to fear and fear arousal itself. *Journal of Advertising*, *26*(3), 45-59.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445-454.

Lee, S., Lee, A. Y., & Kern, M. C. (2011). Viewing time through the lens of the self: The fit effect of self-construal and temporal distance on task perception. *European Journal of Social Psychology*, *41*(2), 191-200.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 77-187.

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for Information Systems*, *12*, 752-780.

Liberman, N., Sagristano, M. D., & Trope, Y. (2002). The effect of temporal distance on level of mental construal. *Journal of Experimental Social Psychology*, *38*(6), 523-534.

Liberman, N., Trope, Y., & Wakslak, C. (2007). Construal level theory and consumer behavior. *Journal of Consumer Psychology*, *17*(2), 113-117.

Liviatan, I., Trope, Y., & Liberman, N. (2008). Interpersonal similarity as a social distance dimension: Implications for perception of others' actions. *Journal of Experimental Social Psychology*, *44*(5), 1256-1269.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469-479.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106-143.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285-311.

Murdock, M. R., & Rajagopal, P. (2017). The sting of social: How emphasizing social consequences in warning messages influences perceptions of risk. *Journal of Marketing*, *81*(2), 83-98.

Nussbaum, S., Trope, Y., & Liberman, N. (2003). Creeping dispositionism: The temporal dynamics of behavior prediction. *Journal of Personality and Social Psychology*, *84*(3), 485-497.

Orazi, D. C., & Pizzetti, M. (2015). Revisiting fear appeals: A structural re-inquiry of the protection motivation model. *International Journal of Research in Marketing*, *32*(2), 223-225.

Orazi, D. C., Lei, J., & Bove, L. L. (2015). The nature and framing of gambling consequences in advertising. *Journal of Business Research*, *68*(10), 2049-2056.

Ponemon Institute. (2017). *2017 cost of data breach study.* Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

Popper, M. (2013). Leaders perceived as distant and close. Some implications for psychological theory on leadership. *The Leadership Quarterly*, *24*(1), 1-8.

Rim, S., Trope, Y., Liberman, N., & Shapira, O. (2013). The highs and lows of mental representation: A construal level perspective on the structure of knowledge. In D E. Carlston (Ed.), *The Oxford handbook of social cognition* (pp. 194-219). New York, NY: Oxford University Press.

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

Sharp. (2017). *Employee IT behaviour highlights GDPR compliance risk.* Retrieved from https://www.sharp.co.uk/cps/rde/xchg/gb/hs.xsl/-/html/employee-it-behaviour-highlights-gdpr-compliance-risk.htm

Shehryar, O., & Hunt, D. M. (2005). A terror management perspective on the persuasiveness of fear appeals. *Journal of Consumer Psychology*, *15*(4), 275-287.

Smith, P. K., & Trope, Y. (2006). You focus on the forest when you're in charge of the trees: Power priming and abstract information processing. *Journal of Personality and Social Psychology*, *90*(4), 578-596.

Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly*, *38*(2), 355-378.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, *13*(2), 147-169.

Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*, 380-427.

Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review*, *117*(2), 440-463.

Trope, Y., Liberman, N., & Wakslak, C. (2007). Construal levels and psychological distance: Effects on representation, prediction, evaluation, and behavior. *Journal of Consumer Psychology*, *17*(2), 83-95.

Ülkümen, G., & Cheema, A. (2011). Framing goals to influence personal savings: The role of specificity and construal level. *Journal of Marketing Research*, *48*(6), 958-969.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, *37*(1), 21-54.

Wakslak, C. J., Trope, Y., Liberman, N., & Alony, R. (2006). Seeing the forest when entry is unlikely: Probability and the mental representation of events. *Journal of Experimental Psychology, 135*(4), 641-653.

Wall, J. D., & Buche, M. W. (2017). To fear or not to fear? A critical review and analysis of fear appeals in the information security context. *Communications of the Association for Information Systems*, *41*, 277-300.

Wall, J. D., & Warkentin, M. (Forthcoming). Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics. *Information & Management*.

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*, *28*(2), 378-396.

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201-218.

Warkentin, M., Walden, E., Johnston, A. C., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems*, *17*(3), 194-215.

White, K., MacDonnell, R., & Dahl, D. W. (2011). It's the mind-set that matters: The role of construal level and message framing in influencing consumer efficacy and conservation behaviors. *Journal of Marketing Research*, *48*(3), 472-485.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse, *MIS Quarterly*, *37*(1), 1-20.

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs*, *61*(2), 113-134.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior*, *27*(5), 591-615.

About the Authors

Davide C. Orazi is an Assistant Professor of Marketing at Monash Business School, Australia. His primary research focus is on persuasion and protection motivation applied to information security, health communications, and social marketing. His research has appeared in *International Journal of Research in Marketing*, *European Journal of Marketing*, *Journal of Business Research*, *International journal of Advertising*, and *Journal of Macromarketing,* among the others. He is one of the winners of the worldwide innovation challenge *Publicis90* based on a digital platform for creative collaboration.

Merrill Warkentin is the James J. Rouse Endowed Professor of Information Systems and a William L. Giles Distinguished Professor in the College of Business at Mississippi State University, and was named an ACM Distinguished Scientist in 2018. His research, primarily on the impacts of organizational, contextual, and dispositional influences on individual behaviors in the contexts of information security, privacy, and social media, has appeared in *MIS Quarterly*, *Journal of MIS*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Information Systems Journal*, *Decision Sciences*, *Communications of the Association for Information Systems*, and others. He is the author of over 90 peer-reviewed journal articles and the author or editor of seven books. He holds or has held editorial roles at *MIS Quarterly*, *Information Systems Research*, *Journal of the AIS*, *Decision Sciences*, *European Journal of Information Systems*, *Information & Management*, and other journals. His work has been funded by NATO, NSF, NSA, DoD, Homeland Security, IBM, and others. He co-founded and chaired the IFIP Working Group on Information Systems Security Research (WG8.11/11.13) and was the Program Co-Chair for the 2016 AIS Americas Conference on Information Systems (AMCIS).

Allen C. Johnston is an Associate Professor of Management Information Systems in the Department of Information Systems, Statistics, and Management Science within the Culverhouse College of Commerce at the University of Alabama. The primary focus of his research is in the areas of behavioral information security, privacy, data loss prevention, collective security, and innovation. His research can be found in such outlets as *MIS Quarterly*, *Journal of the AIS*, *European Journal of Information Systems*, *Information Systems Journal*, *Communications of the ACM*, *Journal of Organizational and End User Computing*, *Information Technology and People*, and *DATABASE for Advances in Information Systems*. He currently serves as AE for *European Journal of Information Systems and Decision Sciences Journal*, as well as serving on the Editorial Review Board for *DATABASE for Advances in Information Systems*. He is a founding member and current Vice Chair of the IFIP Working Group on Information Systems Security Research (WG8.11/11.13).