Communications of the Association for Information Systems

Volume 41 Article 13

9-2017

To Fear or Not to Fear? A Critical Review and Analysis of Fear Appeals in the Information Security Context

Jeffrey D. Wall
School of Business and Economics, Michigan Technological University, jdwall@mtu.edu

Mari W. Buche
Michigan Technological University

Communications of the Association for Information Systems

Research Paper ISSN: 1529-3181

To Fear or Not to Fear? A Critical Review and Analysis of Fear Appeals in the Information Security Context

Jeffrey D. Wall
Michigan Technological University
jdwall@mtu.edu

Mari W. Buche
Michigan Technological University

Abstract:

Controlling organizational insiders' security behaviors is an important management concern. Research presents fear appeals as a viable security control to promote protective security behaviors. To date, research has proven security-related fear appeals have to effectively control insiders' security behaviors. However, from critically examining fear appeals, we find a different story. Specifically, we critically analyze security-related fear appeal research from two ontological positions: critical realism and critical constructivism. The critical realist analysis identifies several issues with existing fear appeal research, which particular research traditions may cause. We explicate these traditions and issues in the paper. The critical constructivist analysis draws on critical management studies of control and Foucault's work to identify the identities, beliefs, and values that fear appeals promote and the ways in which fear appeals create discursive closures that limit the consideration and discussion of other positions. Based on the two analyses, we provide important directions for future fear appeal research.

Keywords: Fear Appeals, Information Security, Protection Motivation, Critical Realism, Critical Management Studies, Critical Literature Review.

This manuscript underwent peer review. It was received 09/30/2016 and was with the authors for 6 months for 2 revisions. Indranil Bose served as Associate Editor.

1 Introduction

Information security continues to be a major management concern (Willison & Warkentin, 2013). Organizations often frame organizational insiders (insiders)—members of an organization, such as employees and board members, with legitimate access to organizational information—as security threats (e.g., Warkentin & Willison, 2009) or assets (e.g., Posey, Roberts, Lowry, Bennett, & Courtney, 2013). Researchers often frame behavioral information security (InfoSec) research as identifying means to "control" these internal human "threats" and "assets" to provide direction for the practice of organizational security control (Wall, Stahl, & Salam, 2015). From a critical management perspective, managers' attempts to frame and control insiders can shape the values and identities of insiders, may lead to discursive closures that limit insiders' perspectives of alternative values and identities, and may even cause psychological and physiological harms and stress to insiders (Deetz, 2003). Organizational security control efforts are not immune to these negative effects. For example, insiders may experience negative reactions to sanctions (Xue, Liang, & Wu, 2011) and computer monitoring (Posey, Bennett, Roberts, & Lowry, 2011). Some insiders perceive these controls to be unfair and unjust, which can result in reactive behavior that damages information security efforts (Posey et al., 2011; Wall, Palvia, & Lowry, 2013). Security controls may also cause stressful conditions that prompt moral disengagement and security violations (D'Arcy, Herath, & Shoss, 2014).

Although behavioral InfoSec research has begun to address the practical tradeoffs of using forceful and invasive security controls such as sanctions and monitoring (Posey et al., 2011; Siponen, 2000), studies that provide a critical perspective on security control deserve further attention. Research and practice do not adequately scrutinize security controls through critical lenses (Stahl, Doherty, & Shaw, 2012), and many studies fail to account for the interests of the insider and instead focus on organizational interests (Wall et al., 2015). From a critical perspective, the failure to account for the interests of all involved actors is a form of discursive closure that limits some actors and ideologies (Deetz, 2003). We need critical analysis in behavioral InfoSec research to extend the representation of different actors and ideologies. Researchers can conduct critical analyses on large and diverse bodies of literature to identify pervasive ideological hegemonies or focus on smaller topical analyses (Wall et al., 2015). Herein, we critically analyze the research and use of a particular topic: fear appeals.

The fear appeal has received increasing attention in behavioral InfoSec research in recent years (Boss, Galletta, Lowry, Moody, & Polak, 2015; Herath & Rao, 2009; Johnston & Warkentin, 2010a; Johnston, Warkentin, & Siponen, 2015). A fear appeal refers to a persuasive tactic that includes a message about a threat and a message about how to cope with the threat (Rogers, 1975). Protection motivation theory (PMT) and fear appeals model (FAM) explain how fear appeals influence security behavior (Johnston et al., 2015; Posey, Roberts, & Lowry, 2016). Although often effective in controlling insiders' security behaviors (Boss et al., 2015; Johnston & Warkentin, 2010a; Johnston et al., 2015), extant research from disciplines such as marketing, communication, politics, and health has questioned the use of fear appeals as motivational drivers (e.g., Hastings, Stead, & Webb, 2004; Ruiter, Kessels, Peters, & Kok, 2014; Wolf, 2007). Behavioral InfoSec research has yet to critically question fear appeals and how they affect insiders and discursive practices in organizations. As such, the prominence of fear appeal research and extant critiques of fear appeals warrants our critically analyzing them.

Drawing from existing security-related fear appeal research, critiques of fear appeals in extant literature, critical management studies, and Foucault's (1977) work on power and discipline, we identify several potential issues with the general study and use of security-related fear appeals. We critically analyze these issues from two different perspectives. Given that existing behavioral InfoSec research is highly positivist in nature (Wall et al., 2015), we first provide critiques from a critical realist perspective. Critical realism adopts a realist ontology, which assumes phenomena exist independently of human perception, and epistemological relativity, which suggests that history and human understand and experience limits knowledge of phenomena (Mingers, Mutch, & Willcocks, 2013). In doing so, we provide guidance for future positivist fear appeal studies. We also offer social and discursive critiques of fear appeals that draw on ontological and epistemological traditions from interpretive and critical research. These critiques cut more deeply into the identities that fear appeals create for insiders and the discursive closures that fear appeals and the larger control environment cause.

This paper proceeds as follows: in Section 2, we present the current state of fear appeal research in behavioral InfoSec literature. In Section 3, we critically analyze existing positivist research from a critical realist perspective to provide directions for future positivist research. We highlight several concepts that

existing studies conspicuously miss and highlight the traditions that have allowed these blind spots to arise. In Section 4, we critically analyze fear appeals from a critical management perspective and focus on how fear appeals create identities for insiders and discursive closures that limit other perspectives of control, information use, and information security. In Section 5, we discuss our findings and directions for future research. Finally, in Section 6, we conclude the paper.

2 Current Fear Appeal Research

Many behavioral InfoSec studies examine fear appeals or theoretical constructs related to fear appeals. The core constructs in the nomology of fear appeal theories include threat appraisals and coping appraisals (Boss et al., 2015). According to fear appeal theories, individuals process and appraise threats specified in fear appeals. Research often represents threat appraisals as individuals' perceptions of threat severity and threat susceptibility or vulnerability (Herath & Rao, 2009; Johnston & Warkentin, 2010a; Johnston et al., 2015). Threat severity refers to individuals' perceptions of how damaging a particular threat is likely to be. Threat susceptibility refers to individuals' perceptions of how likely the threat is to affect them. A more complete representation of threat appraisal also includes maladaptive rewards, which are rewards insiders receive for failing to engage in protective behavior, such as time savings (Boss et al., 2015).

Fear appeals also present individuals with a coping mechanism to counter the threat identified in the message. Coping mechanisms refer to security actions or technologies that organizations ask insiders to use to limit the danger that threats pose. Coping appraisals refer to individuals' beliefs regarding the coping mechanism and the use of it (Rogers, 1983). Fear appeals may seek to alter insiders' appraisals of coping mechanisms to ensure that insiders' appraisals favor the coping mechanism (Johnston & Warkentin, 2010a). Research often represents coping appraisals as response efficacy, response costs, and self-efficacy perceptions (Boss et al., 2015). Response efficacy is an individual's belief that a coping mechanism will reduce a threat. Response costs are perceptions of the personal effort, time, and resources required to respond to the threat by employing the coping mechanism. Self-efficacy refers to the extent to which an individual feels capable of using the coping mechanism to mitigate the threat. More recent behavioral InfoSec research has identified other important fear appeal constructs, which we discuss in Section 2.1.

2.1 Danger and Fear Control Responses

A more complete nomology of fear appeal theories includes fear as a construct and clearly distinguishes between danger control and fear control responses to an appeal (Boss et al., 2015). Researchers believe fear to be the motivational link that drives an individual to adopt a coping mechanism to reduce a threat (Leventhal, 1971; Witte, 1992), but behavioral InfoSec research has often excluded it as an explicit measure (Boss et al., 2015). Fear appeal theories suggest that individuals adopt coping mechanisms to reduce feelings of fear and the negative effects of the associated threat. However, they may adopt coping mechanisms only when they process a fear appeal in a specific way (Witte, 1992).

Individuals may respond to a threat presented in a fear appeal in two ways: through danger control or fear control (Witte, 1992). Danger control refers to individuals' attempts to cope directly with the danger posed by threat to mitigate the threat and reduce threat-related damages. To date, behavioral InfoSec research has focused almost exclusively on danger control. Fear control, an alternative response to fear appeals, refers to individuals' attempts to control fear that do not include directly coping with the threat or threat-related damages. Fear control is another method that individuals employ to reduce fear, such as avoiding fear related messages (Boss et al., 2015). Danger control is likely to lead to protective behavior that reduces a threat. Fear control, however, may result in behavior that increases the negative effects of a threat (Ruiter et al., 2014). Behavioral InfoSec research has yet to adequately explore fear control (Boss et al., 2015).

2.2 Outcome Variables in Fear Appeal Research

In behavioral InfoSec research, fear appeals explain changes in security attitudes (Herath & Rao, 2009), coping and protection motivation (Herath et al., 2014; Posey et al., 2016), behavioral intentions (Johnston et al., 2015; Vance, Siponen, & Pahnila, 2012), and actual security behavior (Ng, Kankanhalli, & Xu, 2009; Workman, Bommer, & Straub, 2008). Researchers have infrequently explored the effects of fear appeals on security attitudes. Herath and Rao (2009) found that threat and coping appraisals improve attitudes

toward security policy. Researchers have also infrequently studied the effects of fear appeals on coping and protection motivation. Threat and coping appraisals improve motivations to adopt coping mechanisms (Boss et al., 2015; Herath et al., 2014). More commonly, behavioral InfoSec research frames the outcome variable in fear appeal studies as behavioral intentions (Johnston & Warkentin, 2010a; Johnston et al., 2015), and a few studies extend intentions to measures of actual behavior (Boss et al., 2015; Workman et al., 2008). These studies show that fear appeals increase intentions to engage in protective security behaviors and increase actual protective behavior. Existing research demonstrates that fear appeals exert substantial impact on insiders' security attitudes, motivations, intentions, and behaviors.

Behavioral InfoSec studies also examine several different security behaviors. Some studies examine security behavior broadly as compliance with information security policy (Herath & Rao, 2009; Siponen, Mahmood, & Pahnila, 2014; Vance et al., 2012) or omissive security behavior (Workman et al., 2008). Other studies focus on one or a few specific security behaviors. Studies have examined behaviors such as anti-spyware adoption (Johnston & Warkentin, 2010a), anti-malware adoption, backup behavior (Boss et al., 2015), email authentication service adoption (Herath et al., 2014), password change behavior, appropriate USB use, system logoff after use (Johnston et al., 2015), and security warning neglecting (Vance, Anderson, Kirwan, & Eargle, 2014). Fear appeal theory has proven useful in explaining many different security behaviors.

To identify clusters and categories of security behaviors relevant to the study of fear appeals, Posey et al. (2013) developed a taxonomy of protection motivation behaviors. The taxonomy relies on three dimensions—degree of criticality, promotion difficulty, and degree of common sense—to form 14 clusters and eight categories of protection motivation behaviors. Degree of criticality refers to the extent to which a behavior is important for all insiders to engage in regardless of their occupation, status, position, or rank (Posey et al., 2013). Promotion difficulty refers to how difficult the behavior is to promote based on the effort required (Posey et al., 2013). Degree of common sense refers to the degree to which insiders perceive a behavior to possess a clear rationale based on their knowledge and experience (Posey et al., 2013). We need more work to understand how fear appeals influence each cluster and category of behavior (Posey et al., 2016).

2.3 Theoretical Configurations of Threat and Coping Appraisals

Behavioral InfoSec research has examined a variety of relationships between threat and coping appraisals and behavior. For example, many studies show threat and coping appraisal constructs to exhibit a direct relationship to an outcome variable, such as behavioral intention (Boss et al., 2015; Vance et al., 2012). Other studies show coping appraisals to mediate or partially mediate the relationship between threat appraisals and an outcome variable (Johnston & Warkentin, 2010a; Johnston et al., 2015), and some also examine threat appraisals as moderating variables (Ng et al., 2009). Still other studies examine antecedents or moderators that influence the effectiveness of threat and coping appraisals (Posey et al., 2016; Vance et al., 2012). Each of these configurations provides a different understanding to the study of fear appeals.

Examining the direct influence of threat and coping appraisals on behavior and behavioral intentions can help one to identify the relative strength and importance of each construct in the model. In health research, several statistical meta-analyses show that strengthening self-efficacy, promoting response efficacy, making individuals aware of their susceptibility to a threat, and avoiding emotional messages about threat severity lead to higher levels of protection motivation (Ruiter et al., 2014). By understanding the relative influence of different constructs, researchers and practitioners may be able to develop persuasive messages that do not rely as heavily on threat and fear (Hastings et al., 2004) but still maintain persuasive power. Examining mediated and partially mediated models helps explain how threat and coping appeals influence one another and interact together to influence insiders' motivations and behavior. By conducting such studies, behavioral InfoSec research has found that threat appraisals influence coping appraisals (Johnston & Warkentin, 2010a; Johnston et al., 2015). However, some inconsistencies exist in the valence of this relationship across studies (see Section 2.4). Studies have also found that threat severity negatively moderates the relationship between self-efficacy and security behavior (Ng et al., 2009). Again, some inconsistencies may exist here as well.

Finally, examining antecedents and moderators of threat and coping appraisals helps explain why fear appeals work well in some contexts but not others. InfoSec research has examined several antecedents to threat and coping appraisal constructs, such as habit (Vance et al., 2012), organizational position (Posey, Roberts, Lowry, & Hightower, 2014), organizational commitment (Herath & Rao, 2009; Posey et

al., 2016), resource availability (Herath & Rao, 2009), and the frequency of security education training and awareness programs (SETA) (Posey et al., 2016). Habit increases threat severity and susceptibility, response efficacy, and self-efficacy and decreases maladaptive rewards and response cost (Vance et al., 2012), which suggests that fear appeals may be more effective for those who already possess strong security habits.

Research has also found that organizational commitment increases response efficacy (Herath & Rao, 2009; Posey et al., 2016), which suggests that fear appeals may be more effective for insiders committed to the organization. Similarly, individuals that receive organizational support, such as accessible security policy and frequent SETA initiatives, are likely to see increases in self-efficacy (Herath & Rao, 2009), response efficacy, and threat severity perceptions (Posey et al., 2016). These findings suggest that fear appeals exert a greater influence on well organizationally supported insiders. These studies show when fear appeals are useful and when they are less useful.

2.4 Empirical Inconsistencies

In general, studies have shown fear appeals to be effective at promoting secure motivations and desirable security behaviors, which explains the relative success and frequency of fear appeal studies in behavioral InfoSec research. However, the literature remains rife with inconsistencies that have yet to be fully resolved. Some studies have found that response efficacy is one of the most influential constructs in promoting secure behavioral intentions (Johnston & Warkentin, 2010a; Johnston et al., 2015). However, other studies have found that response efficacy exhibits a weak correlation with behavioral intention with a negative valence possibly because severity and self-efficacy suppress the true positive valence of response efficacy (Vance et al., 2012). Similarly, studies have found that response efficacy does not exhibit a statistically significant effect on behavioral intentions at all (Siponen et al., 2014).

One possible explanation for the inconsistency is that the studies with low response efficacy had low fear perceptions. Because these studies did not measure fear, we cannot assess this assertion, but future research should consider it. In some cases, the relative effect of response efficacy may decrease when fear appeals do not promote strong fearful feelings (Boss et al., 2015). Thus, measuring fear is important to fear appeal research. Alternatively, the type of protection motivation behavior a study examines could influence response efficacy. For example, protection motivation behaviors low in their degree of common sense (Posey et al., 2013) could result in lower response efficacy beliefs because behaviors low in common sense lack a clear logic and rationale, which are key to the concept of response efficacy.

Similarly, studies have found that self-efficacy strongly and positively influences behavioral intentions (Ng et al., 2009; Vance et al., 2012). Yet, depending on the nature of the self-efficacy task, such as when insiders' high self-efficacy leads them to believe that they can engage in secure behavior without the coping mechanism, self-efficacy may decrease secure behaviors (Herath et al., 2014). Thus, overpromoting self-efficacy in fear appeal messages could potentially backfire. Behavioral InfoSec research does not adequately understand the circumstances under which self-efficacy backfires, and the topic deserves future attention.

Another inconsistency in fear appeal literature is the relationship valence between threat appraisal and coping appraisal. Johnston and Warkentin (2010a) theorized and found that threat appraisals (i.e., threat severity and susceptibility) negatively influence coping appraisals (i.e., self-efficacy and response efficacy). However, other research has found that threat appraisals positively influence coping appraisals (Herath et al., 2014; Johnston et al., 2015). Herath et al.'s (2014) alternative operationalizations for threat appraisal and coping appraisal could explain the difference: these authors operationalized threat appraisal as risk perceptions and coping appraisal as the usefulness of the coping mechanism. However, this operationalization does not explain the disparate findings between Johnston and Warkentin (2010a) and Johnston et al. (2015), which both employed similar operationalizations of threat and coping appraisals. Again, the different types of behavior examined in each study could explain the differences. Further replication is needed to explain this inconsistency.

Ng et al. (2009) and Boss et al. (2015) also present seemingly inconsistent findings. Ng et al. (2009) found that, as threat severity increases, the relationship between self-efficacy and security behavior weakens. That is, self-efficacy influences behavior less when threat severity is high. Conversely, Boss et al. (2015) designed high and low fear appeal manipulations. They found that the high fear appeal manipulation increased severity perceptions more than the low fear appeal manipulation. Under the high fear appeal manipulation, which resulted in stronger severity perceptions, self-efficacy positively influenced behavioral

intentions. However, under the low fear appeal manipulation, which resulted in lower severity perceptions, self-efficacy did not exhibit a statistically significant effect or exhibited a negative effect on behavioral intentions (Boss et al., 2015). One cannot directly compare the studies because they adopt different approaches (i.e., moderation vs. experimental manipulation). However, this potential discrepancy deserves further exploration. Again, the measurement of different protection motivation behaviors across the studies may account for the differences. We need further replications to understand the relationship between threat severity and self-efficacy.

3 A Critical Realist Critique

In this section, we critique security-related fear appeals from a critical realist perspective. Critical realism suggests that, due to history and contextual understandings of phenomena, researchers will not always be attentive to all concepts and factors surrounding the study of a phenomenon. Thus, researchers' understandings of real phenomenon may be biased or incomplete. We identify some of these incomplete conceptions of fear appeals to advance research in the area. We also present important research questions to examine in future positivistic research.

3.1 Studying Fear Control

Although behavioral InfoSec research has continued to expand the nomology of fear appeal theories (Boss et al., 2015), it has not adequately addressed some core concepts. Most concerning is the lack of research that examines fear control. In a security context, fear control could manifest itself in various ways. For example, some insiders who act under fear control could avoid security-related messages. Other insiders might seek out alternative messaging to downplay the existence or severity of security threats. It may also be possible that insiders neutralize fear appeals similar to the way they neutralize sanctions, such as blaming consumers for sharing their information with organizations or blaming organizations for collecting private data. These examples are all theoretical and ontological possibilities that existing research has not addressed. Importantly, fear control may lead to negligent behavior caused by a failure to engage with fear appeal messages and can result in other counterproductive behaviors (Hastings et al., 2004). The possibility that fear appeals in a security context could lead to negligent behavior or security violations is of great concern to management.

Research's failure to study fear control has created a blind spot due possibly to a fixation on positive outcome variables (e.g., protective security behavior) that future research must address. It can do so in several ways. For example, studies can include measures of possible fear control responses (e.g., avoiding security messages and seeking alternative viewpoints) alongside measures of danger control responses (e.g., protective attitudes, motivations, intentions, and behaviors). Studying fear and danger control together could suggest whether insiders experience both control responses simultaneously and could explain the circumstances under which each response is likely to dominate actual behavior. Alternatively, studies could examine negative security behaviors, such as information security policy violations or computer abuse, instead of protective behaviors. In such studies, the theoretical emphasis would focus on explaining how and why fear control is activated and whether it leads to negligent or damaging security behavior.

From the core nomology of fear appeal theories, maladaptive rewards presents an obvious construct that could explain why individuals engage in fear control instead of danger control. Beyond maladaptive rewards, existing behavioral InfoSec research may contain key concepts to explain the conditions under which fear control and not danger control is likely to dominate behavior. The effectiveness of fear appeals, from a danger control perspective, is influenced by habit (Vance et al., 2012), organizational position (Posey et al., 2014), organizational commitment (Herath & Rao, 2009; Posey et al., 2016), and organizational support (Herath & Rao, 2009; Posey et al., 2016). These same concepts that explain why insiders are more likely to engage in danger control may provide important insight in studying fear control simply by reversing the valence of the constructs studied in danger control studies. For example, poor security habits, low organizational commitment, and weak organizational support might increase fear control responses to fear appeals. Future research should test these ideas.

Extant literature may also contain noteworthy concepts. Extant fear appeal studies suggest that recipients of fear appeals in real-world situations may give less attention to fear appeal messages than under experimental conditions (Hastings et al., 2004). Individuals and organizations have limited attentional resources and must be selective in the issues they attend to (Carrier & Prashler, 1995; Wall, Lowry, &

Barlow, 2016). Individuals can easily tune out marketing messages that use fear appeals (Hastings et al., 2004). If individuals improperly process fear appeals due to low attention, fear control could be possible. Thus, future research should study attention to fear appeals. If one examined danger and fear control in a single study, one could include the above factors as moderating variables between fear and coping appraisals and behavioral outcomes. Understanding interaction effects that these factors cause could explain why fear appeals sometimes result in danger control and other times do not. Figure 1 presents one possible configuration to study the link between fear and danger and fear control responses. Based on this discussion, future positivist research should seek to answer the following questions:

RQ1a: What individual and organizational factors influence the adoption of fear control responses as compared to danger control responses in security contexts?

RQ1b: Do fear control responses to fear appeals lead to negligent or damaging security behavior?

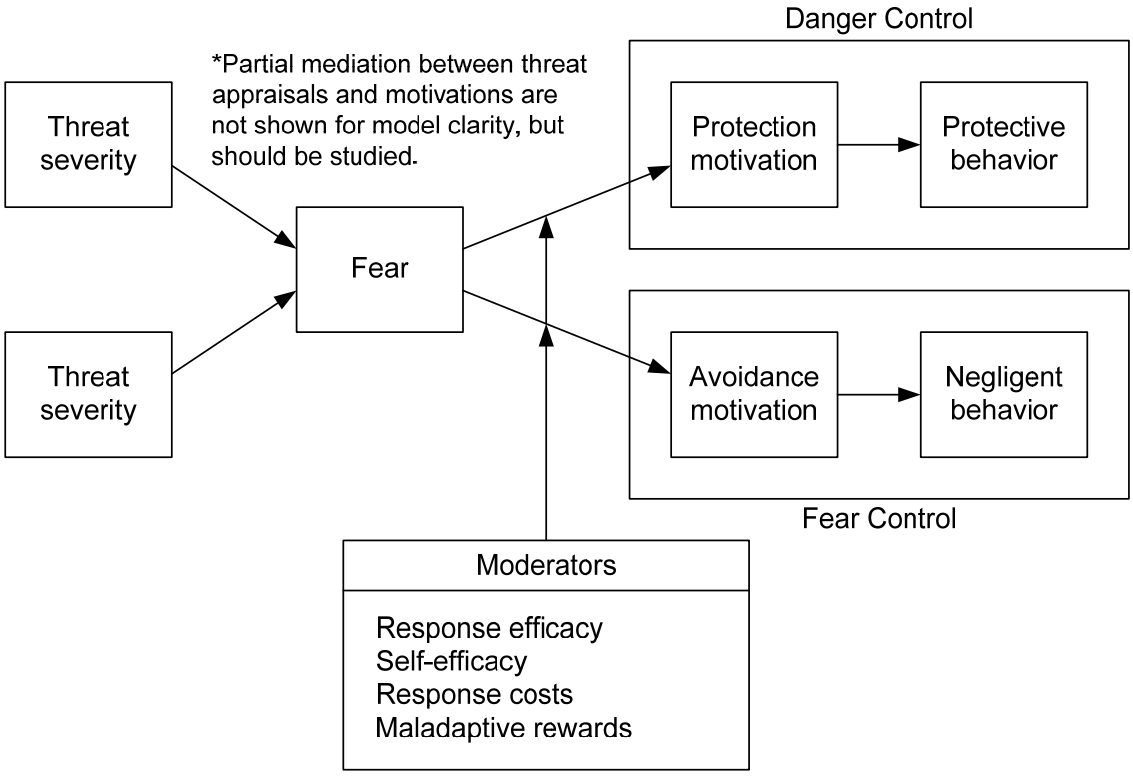

Figure 1. Fear Appeal Nomology Including Fear Control

3.2 Studying Antecedents of Fear and Coping Appraisals

Researchers have criticized behavioral InfoSec research and information systems research in general for relying too much on reference disciplines for theoretical guidance (Baskerville & Myers, 2002; Crossler et al., 2013; Wall et al., 2015). Behavioral InfoSec research has adopted several theories, such as deterrence theory, protection motivation theory, and control theory. Although adopting extant theories is not inherently bad or wrong, it can limit perceptions of phenomena. Extant fear appeal theories propose a set of predefined concepts for study. As we suggest in Section 3.1, behavioral InfoSec research has yet to adopt the complete nomology of fear appeal theories. But even if researchers do adopt additional concepts, the complete fear appeal nomology will still represent a historical understanding of fear appeals. From a critical realist perspective, behavioral InfoSec research should continue to refine and extend understandings of the concepts that are important to studying fear appeals. Some security studies have begun this crucial research process. The consideration of antecedents to threat and coping appraisals in existing research provides evidence of the continued refinement of fear appeal concepts, which is laudable. However, researchers borrowed many of these concepts from other extant theories.

Fear appeal research could benefit substantially from more qualitative research that focuses on understanding insiders' perceptions and reactions to fear appeals. Qualitative research is noted for its

ability to define new concepts (Corbin & Strauss, 1990), and some strains of qualitative research adopt positivistic ontological notions of realism (Lee, 1989; Yin, 2002) that could complement the current positivist fear appeal regime. The dominance of theory adoption and quantitative analysis in behavioral InfoSec research has limited its considering novel fear appeal constructs. We call for more qualitative studies that examine additional factors that influence the effectiveness of fear appeals. Qualitative studies may also provide insight into when individuals adopt danger control and fear control responses.

Researchers have also critiqued IS research for its lack of relevance to management practice (Dennis, 2001). A hyper focus on parsimonious theory can sometimes lead to theories with obvious notions, such as the notion that individuals will be more likely to use systems that are useful and easy to use. Current fear appeal studies are somewhat constrained to the same obvious, high-level notions. At its core, fear appeal theory states that fear can be manipulated, that individuals seek to minimize their fear of threats and threat related damages, and that individuals are likely to adopt quality coping mechanism that will mitigate the threat to reduce the fear. Often missing from fear appeal studies are concepts that describe how one can effectively manipulate fear or how one can influence coping appraisals to ensure individuals adopt coping mechanisms. These questions are crucial to management practice and may add greater relevance to fear appeal research.

Behavioral InfoSec research has primarily grounded itself in the management discipline by focusing on concepts that assist managers in understanding and controlling insider security behavior. Thus, one should expect some amount of management relevance in security-related fear appeal research. Some security-related fear appeal studies have moved in this direction. For example, findings that organizational support influences threat and coping appraisals (Herath & Rao, 2009; Posey et al., 2016) provide actionable direction for managers. Two obvious sets of factors that the existing literature does not adequately address and that could increase research relevance include factors related to the message or message framing in a fear appeal. Fear appeals are ultimately persuasive messages that managers craft and disseminate. Truly relevant fear appeal research should explain how managers can better frame messages to alter threat and coping appraisals. Theories of message framing and persuasion may provide additional insight into how managers can construct quality fear appeals. Again, qualitative studies of insiders' perceptions of fear appeal messages may provide important insight.

Some theories that may provide insight include prospect theory and the elaboration likelihood model. Prospect theory (Kahneman & Tversky, 1979) suggests that individuals' perceptions of risk differ based on whether a message is framed in terms of a loss or in terms of a gain. Healthcare research uses prospect theory, similar to protection motivation theory, to explain adherence to medical recommendations (Rotham, Salovey, Antone, Keough, & Martin, 1993; Van't Riet et al., 2016). Risk is paramount to fear appeal theories as represented by threat appraisals. Thus, prospect theory and fear appeal theories seem to have some compatibility. Understanding how the loss or gain framing of fear appeals influences threat appraisals could provide relevant fear appeal design guidance for managers. The elaboration likelihood model (Petty & Cacioppo, 1986) is a theory of persuasion that identifies the conditions under which an individual will expend cognitive resources to carefully process a message, which increases the likelihood they will change their attitudes and behaviors. The elaboration likelihood model suggests that high-quality arguments in a message increase the likelihood that individuals will carefully process the message and change their behavior (Petty & Cacioppo, 1986). Understanding how argument quality influences threat and coping appraisals could also provide further actionable information to managers. Figure 2 presents an extension of fear appeals nomology and focuses on antecedents of threat and coping appraisals. Based on this discussion, we suggest the following research questions:

RQ2a: What concepts explain the effectiveness of fear appeals beyond the core nomology of concepts that fear appeal theories prescribe?

RQ2b: What characteristics of a fear appeal message, such as argument quality and loss and gain framing, explain the effectiveness of fear appeals?

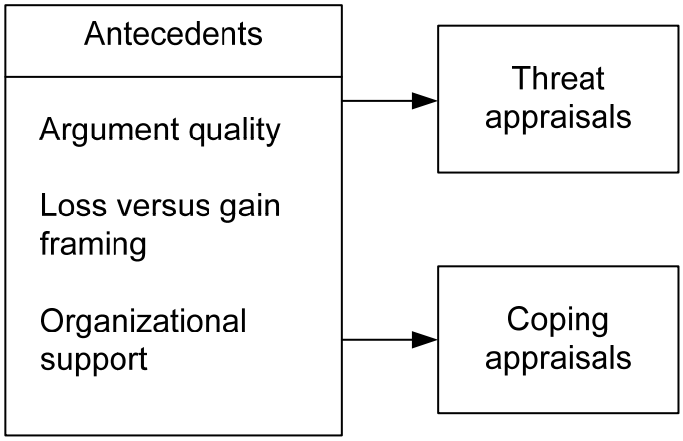

Figure 2. Example of Fear Appeal Nomology with Management-relevant Antecedents

3.3 Considering Insider-centric Outcome Variables

Because of the management-centric focus in behavioral InfoSec research, outcome variables in security-related fear appeal studies primarily target organizational interests (Wall et al., 2015) (namely, compliance with information security policy or protective security behavior). The management-centric focus of existing research has blinded researchers to the fact that insiders have their own interests that do not necessarily complement organizational interests (Deetz, 2003). Existing research does not give insiders' interests, such as a quality work environment, mental health, fairness, and respect, the same prominence as organizational interests.

The extant literature often criticizes fear appeals for the negative emotions and feelings they instill in individuals (Hastings et al., 2004; Wolf, 2007). Fear appeal research shows, though sometimes inconsistently, that fear and negative emotions can be strong motivators (Ruiter et al., 2014). However, excessive fear is also associated with maladaptive responses to fear appeals (Peters, Ruiter, & Kok, 2012). When individuals feel unable to cope with fear, such as when they experience low self-efficacy, they may ignore coping messages and engage in threatening behaviors (Peters et al., 2012; Ruiter et al., 2014). Fear appeals may also produce negative affect beyond fear, such as depression and anxiety related to a threat (Das, de Wit, & Stroebe, 2003). Similar to the effects of fear, negative affect further increases persuasion (Das et al., 2003); however, negative emotions experienced in the workplace are also associated with counterproductive work behavior (Fida et al., 2015). Negative emotion is related to turnover intentions in the workplace as well (Wright & Cropanzano, 1998). Turnover intentions can lead to moral disengagement among employees and, thus, to deviant behavior at work (Christian & Ellis, 2014).

Relying on coping theory, behavioral InfoSec research has found that negative emotions, such as security-related stress, can lead to moral disengagement and intentions to violate information security policy (D'Arcy et al., 2014). It has also shown negative feelings, such as injustice perceptions, to increase insiders' computer abuse behaviors (Posey et al., 2011) and decrease compliance intentions (Xue et al., 2011). Reactance theory also shows how certain individuals are prone to react to organizational attempts to control them (Wall et al., 2013). Clearly, negative emotions influence insiders in the information security context in a similar fashion to other contexts. To include insider interests in fear appeal research, future positivist fear appeal studies should explore outcome variables such as stress, satisfaction, reactance, injustice perceptions, fear, moral disengagement, and turnover intentions. If fear appeals lead to other negative emotions that cause moral disengagement and security violations, managers should question the use of fear appeals as a security control mechanism. Figure 3 presents a nomology of fear appeals concerned with insider-centric outcomes. Based on this discussion, we suggest the following research question:

RQ3: How do fear appeals affect insiders' wellbeing (e.g., job satisfaction, stress, and reactance)?

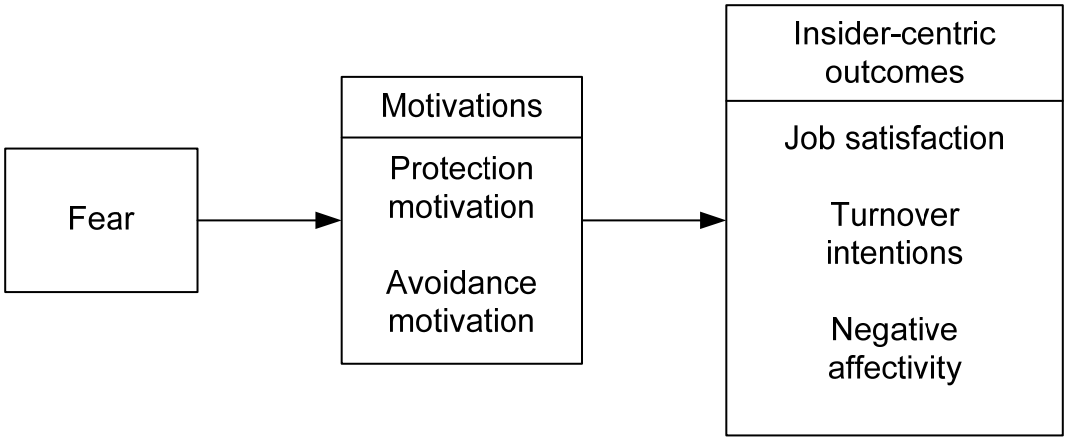

Figure 3. Example of Insider-centric Fear Appeal Nomology

3.4 Examining the Long-term Effects and Use of Fear Appeals

Behavioral InfoSec research primarily comprises cross-sectional quantitative studies (Wall et al., 2015). This historical norm has led to studies that examine fear appeals at a single point in time, which may be a blind spot in the long-term use of fear appeals in practice. Extant research criticizes fear appeals by suggesting that the motivating effect of an individual fear appeal is short-lived, which requires practitioners to adopt fear campaigns that may necessitate the continual increase of the fear level in each subsequent appeal (Hastings et al., 2004). Behavioral InfoSec research has also acknowledged that fear appeals require multiple applications through a campaign (Boss et al., 2015). Few studies in extant literature employ repeated measures of fear (Dillard, Li, Meczkowski, Yang, & Shen, 2016), and no study to our knowledge has examined repeated measures over a long period. Although Boss et al. (2015) employed a longitudinal study, they measured fear only at one time point (i.e., after they presented the last fear appeal). Single, static measures of fear in longitudinal studies may underestimate peak fear levels and overestimate end fear levels (Dillard et al., 2016). We do not understand the effects of fear over time well (Dillard et al., forthcoming); thus, such effects deserve future research attention.

Fear appeal campaigns and the possibility that fear must be continually increased over the length of a campaign add further questions to the usefulness of fear appeals as a security control. Recent behavioral InfoSec research suggests that fear may need to be high for fear appeals to be effective (Boss et al., 2015). When fear appeals exert low fear on insiders, fear may actually decrease behavioral intentions and reverse the positive effect of self-efficacy on behavioral intentions in some situations (Boss et al., 2015). If the effectiveness of fear appeals is inconsistent and limited to certain populations, fear appeals may not be a strong control in practice. It is essential to address the longitudinal effect of fear that fear appeals produce and to determine whether fear appeal messages increasingly desensitize individuals over time. Based on this discussion, we suggest the following questions:

RQ4a: How effective are longer-term fear appeal campaigns?

RQ4b: Do security-related fear appeals become less effective over time due to insider desensitization?

3.5 Summary of Critical Realist Critiques

In this section, we explicate several issues in positivist security-related fear appeal research. Using critical realism, we describe several traditions and historical factors that have limited fear appeal research. Table 1 presents the possible issues that currently exist in the study and practice of fear appeals.

Table 1. Summary of Critical Realist Critiques

Issue	Description	Limiting traditions and practices	Directions for future research
Contradictory findings	The valence or statistical significance of some relationships in the fear appeal nomology differs across study results.	Caused by the lack of replication studies—possibly due to norms of publishing novel research.	Many of the contradictory findings exist between only two studies. We need replication research to understand why these discrepancies exist.
Fear control unstudied	Fear control is a crucial element of fear appeal nomology, but fear appeal research has not yet studied it.	May be caused by a fixation on protective behaviors because of the adoption of protection motivation theory.	Research must understand the conditions under which fear appeal responses will dominate danger control responses and whether fear control leads to negligent and damaging security behavior.
Restrictive set of concepts	Fear appeal research focuses mostly on concepts studied in extant fields.	May be caused by norms of theory borrowing and a heavy focus on quantitative research methods.	Research should continue to extend the nomology of fear appeal theories. Qualitative studies may provide useful insight into new and important constructs.
Management relevance	Many fear appeal concepts are at a high level and do not provide actionable detail for managers.	May be caused by norms of theory borrowing and a fixation on theoretical parsimony.	Research should examine aspects of fear appeal messages and message framing that will assist managers in designing more effective fear appeals.
Management-centric outcomes	Fear appeal research outcomes are almost exclusively management centric (i.e., promoting protective behavior).	May be caused by the management-centric tradition of behavioral InfoSec research.	Research should consider insider-centric outcome variables, such as satisfaction, affectivity, stress, and turnover intentions.
Short-term research focus	Fear appeals effects may not last long and may require a constant elevation of fear levels.	May be caused by traditions of conducting cross-sectional studies in behavioral InfoSec research.	We need longitudinal studies with multiple measures of fear and protection motivation.

The research findings we present thus far subtly question the effectiveness of fear appeals. For example, fear appeals may only work well when fear is high (Boss et al., 2015), when insiders are committed to their organizations (Posey et al., 2016), when organizations train and support insiders well (Herath & Rao, 2009; Posey et al., 2016), and when insiders already have strong security habits (Vance et al., 2012). Fear appeals could also possible work differently for different protection-motivation behaviors (Posey et al., 2013). Further, several disparate findings remain mostly unanswered, such as the effect of threat appraisals on coping appraisals (Johnston & Warkentin, 2010a; Johnston et al., 2015) and disparate findings regarding the importance of self-efficacy and response efficacy. Fear appeals may also result in fear control, which could lead to negligent or damaging security behavior.

Considered separately, each study generally shows positive security outcomes from the use of fear appeals. However, looking across the studies paints a picture of an increasingly limited and possibly inconsistent security control. Given that fear appeals promote and feed on negative emotions and cognitions, such as fear, the limits of fear appeals should cause researchers to question whether organizations should use these appeals to promote secure behavior. Positivist research should seek to answer the questions we present in Sections 3.1 to 3.4 to identify conditions that lead to danger control and those that lead to fear control. Research should also seek to identify important antecedents and moderating factors that can assist managers in developing strong fear appeals with consistent results. Finally, researchers should carefully consider insiders' interests and weigh them against the organization's interests to determine the value of fear appeals as a security control mechanism. If future research cannot provide insight into creating fear appeals that produce consistent and effective control results, researchers should not tout fear appeals as a viable control mechanism.

4 A Critical Management Critique

In this paper thus far, we examine fear appeals and fear appeal research from a positivist perspective using critical realism. However, critical management studies and Foucault's (1977) work on power and discipline present a different set of critiques based on critical and interpretive research paradigms. From a critical and interpretive perspective, the ontology of control and its relationships to human perception and behavior do not represent a fixed reality that exists independent of human perception. Rather, ontologically speaking, control is a social construction that individuals constantly reify through discursive practices or punishment (Deetz, 2003; Klein & Myers, 1999; Myers & Klein, 2011). Thus, control is maintained as individuals agree, consciously or unconsciously, to the rules, norms, and ideologies of those who seek to establish control. Critical management studies focus on understanding the multiple and sometimes conflicting interests of organizations and insiders and on critiquing how organizations exercise power to ensure that organizational interests take precedence over insider interests (Deetz, 2003).

Foucault (1977) distinguishes between two forms of control (namely, punishment and discipline) that governing bodies employ to pursue their interest at the expense of others' interests. Punishment relies on exercising force, coercion, and sometimes violence to align individuals' behaviors with the desires of those that set themselves as legitimate powers through using said punishment. Discipline relies on discursive practices and structures that limit the perspectives of those being controlled and that normalize behaviors that favor the interests of those who exercise control. Organizations primarily rely on discipline to align insider behavior with organizational interests. In organizations, discipline takes the form of organizational practices and structures such as policies, procedures, training, hierarchies, and job specialization (Deetz, 2003; Stahl, 2008). These practices and structures are embedded in the fabric of organizational life and may become invisible to insiders (March & Simon, 1958). Organizations often use punishment, such as threats of termination or sanctions, when disciplinary practices break down (Deetz, 2003).

The structures and discursive practices that organizations employ may create specific identities for insiders and set forth a set of beliefs and values that the organizations expect insiders to follow (Deetz, 2003). Identities emerge when different actors use language to distinguish themselves from each other, such as the distinction between manager and employee. It is these identities, beliefs, and values that we critique—particularly when organizations use discipline to create discursive closures that limit insiders from considering other meaningful and relevant identities, beliefs, and values. The use of fear appeals represents a discursive practice that organizations employ to establish specific identities for insiders and normalize certain beliefs and values. We analyze these identities, beliefs, and values and the ways in which fear appeals create discursive closures that limit the consideration of other identities, beliefs, and values in research and in practice.

4.1 Fear Appeals and Insider Identity, Beliefs, and Values

As protection motivation theory's name suggests, fear appeals seek to create an identity for insiders as "protectors" of customers' private information and the organizations' proprietary information. Thus, insiders are subjected as "protectors" and customers and organizational information are subjected as "the protected". Individuals form these identities by adopting the discursive logics contained in fear appeals. As a persuasive tactic, fear appeals seek to alter insiders' perceptions of organizational realities by specifying a threat to some entity that insiders can thwart through using some security practice or technology that will protect against the threat (Boss et al., 2015). Each time managers disseminate a fear appeal that insiders accept, the insiders reify their identity as a protector. Fear appeals are just one of many security controls that paint insiders as protectors and customers and organizational information as the protected. Security education awareness and training programs, for example, attempt to persuade individuals about the importance of protecting information and to specify insider responsibilities in protecting private and proprietary information (Puhakainen & Siponen, 2010). Security policies also specify insiders' protective responsibilities and what they should protect. Together, these controls help to reiterate the protective identities that organizations desire.

When these discursive practices fail, organizations employ sanctions to punish violators (Deetz, 2003), which further incentivizes insiders to adopt the protector identity to avoid further punishment. If repeated punishment fails, organizations may terminate insiders and select new ones who ideally have beliefs and values that already favor the protector identity. Selection during the hiring process is a common form of control that organizations adopt to ensure that insiders' identities align with organization interests

(Eisenhardt, 1985; Ouchi, 1977). These various control mechanisms help to ensure that the protector and the protected identities become natural and that insiders perceive them as neutral.

The protector identity brings with it a set of beliefs and values. Some of these beliefs and values may be explicit, while others may be hidden and taken for granted. The protector identity likely carries with it beliefs that organizations are stewards of others' information and have the right to control how insiders use it the information because the protector identity assumes that there must be something to protect. The protector identity may also support the belief that certain information that organizations produce is proprietary and belongs to the organization (i.e., the protected). The protector identity may promote values of security, a form of privacy that grants organizations control over what constitutes acceptable disclosure of information and use of information assets. Although there is nothing inherently bad or wrong with promoting the protector/protected identities or their associated beliefs and values, organizations that do so can create discursive closures that limit employees from considering other valid identities, beliefs, and values. Research does not well document the protector identity and its associated beliefs. The ideas we present about the protector identity are based on the persuasive logics that fear appeal messages employ. Future research should seek to understand the lived experiences of individuals subjected to security-related fear appeals to richly identify the associated identities, beliefs, and values that form from the use of fear appeals. Based on this discussion, we suggest the following research questions:

RQ5a: What are the lived experiences of those subjected to security-related fear appeals?

RQ5b: What identities, beliefs, and values do those subjected to security-related fear appeals embrace?

4.2 Fear Appeals and Discursive Closures

Discursive closure may occur when an organization employs pervasive discipline that supports a single or small set of identities, beliefs, and values to the exclusion of other legitimate positions (Deetz, 2003). Such practices and the resulting discursive closures are undemocratic. Democracy in the form of the free expression of ideas is a cornerstone of many critical theories (Habermas, 1979, 1984). Critical research seeks to identify and challenge undemocratic practices that limit or ostracize different ways of thinking and acting (Myers & Klein, 2011).

Fear appeals can create discursive closures (Glassner, 2009). For example, fear appeals and related controls may promote the protector identity. In doing so, fear appeals may inherently promote the beliefs of the protector identity, such as the acceptance of organizations as rightful stewards of consumer information and insiders as the protectors of that information. Despite the singularity of the beliefs and values that security-related fear appeals and related controls may establish, beliefs about the ownership of consumer information are far from singular. Many believe that governments and organizations should not be allowed to own and control consumer information (Al-Khouri, 2012; Hogan & Shepherd, 2015). Further, researchers and practitioners continue to develop technologies, such as the blockchain, to ensure that consumers can maintain control over their own information (Zyskind, Nathan, & Pentland, 2015). Pervasive security controls, such as fear appeals, may limit insiders' opportunities to voice concerns over the use of consumer data in the organization by normalizing the protector identity and its associated beliefs and values.

To the extent that insiders adopt the protector identity, its beliefs and values may also bleed into their lives as consumers. Pervasive discourses easily spread to all aspects of life (Deetz, 2003); thus, managers must take care when discussing protectors and the protected. Consumers controlled by the pervasive protector identity in the workplace may not know about alternative positions or feel helpless to combat ubiquitous information ownership norms.

Further, fear appeals can distract individuals from larger and more systemic issues (Glassner, 2009). Individuals have a limited attentional capacity, and organizations and politicians regularly use fear to draw individuals' attention away from substantive issues and toward menial ones (Glassner, 2009). Organizations could easily use fear appeals in the security context to distract insiders from larger debates over information ownership and, thus, create discursive closures.

Fear appeal research demonstrates that stronger fear appeals increases response efficacy perceptions by increasing threat appraisals and fear (Boss et al., 2015). Fear appeal theories assert that response efficacy perceptions increase because fear drives individuals to pay closer attention to the messages about the coping mechanism that the fear appeal presents (Ruiter et al., 2014). This assertion assumes,

however, that the fear appeal presents a truly efficacious coping mechanism. Organizations can use fear appeals to increase perceptions of response efficacy, and such appeals can lead to individuals' adopting coping mechanisms that are not actually efficacious in practice (Glassner, 2009). Organizations may also use organizational and security controls to demonstrate symbolic compliance with governmental regulations or industry norms (Lehman & Ramanujam, 2009; Wall et al., 2016). Thus, in practice, fear appeals may act as a symbolic gesture to suggest that organizations care about privacy, even though their actual behaviors violate it. This practice is another way in which organizations may engage in insincere communication and, thus, create discursive closures. From a critical management perspective, organizations should question their engagement in practices that create discursive closures. Thus, we call for further research to assess the power of fear appeals and related security controls to create discursive closures, particularly around the debate of information ownership. Based on this discussion, we suggest the following research questions:

RQ6a: How do fear appeals and related security controls create discursive closures in organizations?

RQ6b: Do the identities, beliefs, and values that insiders learn through security-related fear appeals in the workplace influence their identities, beliefs, and values of information ownership as consumers?

RQ6c: What policies and practices can organizations adopt to prevent discursive closures regarding information ownership**?**

RQ6d: Do organizations use fear appeals and other security controls to hide their privacy-violating behavior, and what conditions prompt them to do so?

4.3 Power, Control, and Vulnerable Insiders

Critical studies frequently question organizations' exercising power and control over vulnerable individuals. For example, the Nuremberg Code introduced the idea of voluntary consent in research. Similarly, institutional review boards seek to protect the rights of children, prisoners, and other vulnerable groups. Organizations are also subjected to human resource laws that limit the power that they may exercise over insiders. Organizations and researchers should carefully consider the insiders who may be particularly vulnerable to fear appeals.

Extant critiques of fear appeals draw attention to vulnerable groups that fear appeals intentionally or unintentionally affect. For example, some researchers call for further research on the effects of fear appeals on elderly individuals to ensure that researchers use fear appeals ethically on elderly populations (Hastings et al., 2004). Some individuals may also be prone to negative affectivity as a character trait, which may include heightened sensitivity to fear and punishment (Thoresen, Kaplan, Barsky, Warren, & de Chermont, 2003). Thus, fear appeals may be particularly harmful to individuals prone toward negative affectivity. Considering how a fear appeal affects vulnerable populations is an important step in identifying how to ethically use fear appeals.

Researchers have further criticized fear appeals for being counterproductive for the individuals who could benefit the most from the coping mechanisms they present. Those who most need the coping mechanism, those most vulnerable to the threat, may be more likely to engage in fear control and maladaptive behavior or may be ostracized for failing to engage in adaptive behaviors (Hastings et al., 2004). For example, meta-analytic studies in health research have demonstrated that individuals with low self-efficacy are more likely to continue threatening behavior and may even worsen their health-related behavior (Ruiter et al., 2014). Behavioral InfoSec research has implicitly identified several potentially vulnerable insiders. For example, individuals with low organizational commitment are not as likely to engage in danger control when presented with fear appeals (Posey et al., 2016). Non-committed insiders could, therefore, be more likely to engage in fear control and maladaptive behaviors.

Insiders with poor security habits may also be less likely to employ danger control responses than insiders with strong security habits. For example, insiders with strong security habits are influenced by fear appeals more than insiders with poor security habits (Vance et al., 2012). Finally, insiders with low security self-efficacy may be at risk. Low self-efficacy may lead to fear control and maladaptive behavior (Ruiter et al., 2014). Thus, users who feel incapable of completing certain security tasks may ignore security-related fear appeals and may even engage in further threatening security behaviors. These ideas suggest that the individuals who most need the influence of fear appeals (i.e., uncommitted insiders with

low self-efficacy and poor security habits) may be the least likely to be persuaded by them. These vulnerable insiders already possess attributes that make them security threats to the organization (e.g., low organizational commitment). If fear appeals cannot help the most vulnerable insiders and if they even worsen their behaviors, they may be inappropriate as a form of security control. That is, if fear appeals do not meet organizational interests and cause unnecessary stress and discomfort to insiders, organizations should strongly question their use. Based on this discussion, we suggest the following research questions:

RQ7a: What types of insiders do fear appeals disproportionally affect in negative ways in the information security context?

RQ7b: Do the protective benefits of fear appeals outweigh the potential harms and possible counterproductive behaviors that fear appeals cause?

4.4 Summary of Critical Management Critiques

In Sections 4.1 to 4.3, we identify several critical management issues related to the use of security-related fear appeals and other security controls that future research and management practice should consider. Table 2 presents the critical insights that future research should address.

Table 2. Summary of Critical Management Critiques

Critical insight	Description	Directions for future research
Formation of identities, beliefs, and values	The persuasive logic of fear appeals and related security controls create identities for insiders, customers, and organizational information; namely, that of protector and the protected. These identities are imbued with specific beliefs and values.	Research should seek to understand the lived experiences of insiders as they interact with security controls, such as fear appeals. Research should richly identify the identities that fear appeals form and the beliefs and values associated with those identities.
Discursive closures	Pervasive fear appeals alongside other security controls may create discursive closures that limit individuals from forming other identities and hamper them from openly discussing other beliefs and values, such as information ownership rights.	Research should seek to understand, through insiders' experience, what identities related to the use and ownership of information organizations allow. Following in the critical tradition, research should also identify ways to democratize discussions of information-related issues (e.g., information ownership).
Use of control as a symbolic gesture	Organizations may use controls to symbolically demonstrate a willingness to comply with government or consumer standards, such as privacy standards. However, at times, organizational practices may actually contradict their symbolic displays of compliance.	Research should examine the factors that prompt organizations to use symbolic gestures to hide controversial behaviors. Fear appeals may be just one of many symbolic gestures.
Vulnerable insiders	Some insiders may be more vulnerable to the negative effects of fear appeals, such as those prone to negative affectivity. Fear appeals may also lead to fear control for those most in need of the coping mechanisms that fear appeals present.	Research should begin to identify vulnerable insiders. Studying the lived experiences of insiders will begin to identify characteristics of insiders that are most vulnerable to fear control and other negative effects. Research should carefully weigh the human costs of fear appeals, the damage fear control causes, and the benefits that danger control causes.

Control is an inevitability (Deetz, 2003; Foucault, 1977), but it does not have to be one sided. Fear appeals and other security controls provide a limited set of identities and purport a specific set of beliefs and values. When left undiscussed and unchallenged, these identities, beliefs, and values become natural and neutral to those under their control. Managers themselves may even be unaware of the identities, beliefs, and values they assume by using fear appeals. Organizations and insiders should seek to open discussions about the use of fear appeals and other security controls. Controversial subjects such as information ownership and the use of private data should not go undebated. From a critical management perspective, organizations should grant insiders some leeway in considering and discussing different identities, beliefs, and values.

5 Discussion

Fear appeals have come under scrutiny in many disciplines. Extent research has identified fear appeals as a harsh and sometimes ineffective form of control (Hastings et al., 2004; Ruiter et al., 2014). Drawing on extant critiques of fear appeals, existing security-related fear appeal research, critical realism, and critical management studies, we comprehensively critically analyze fear appeals from two ontological positions. By relying on critical realism as a foundation for part of our analysis, we identify important directions for future positivist fear appeal research. We also identify how certain research traditions (e.g., a historical focus on cross-sectional, management-centric, quantitative studies) have led to specific blind spots in positivist fear appeal research. By considering critical management studies with a social constructivist ontology, we analyze the discursive practices surrounding the use of fear appeals and the discursive closures they cause.

5.1 Reflexivity

In critical research and in critical reviews, reflexivity is paramount (Stahl, 2008; Wall et al., 2015). Thus, in this section, we reflexively analyze the positions we present in this paper. Researchers deeply steeped in either social constructivist or realist ontological traditions may find it odd to include critical realist critiques alongside social constructivist critiques. Critical analyses often assume a singular ontological perspective. However, we do not feel deeply or singly connected to any particular ontological position. We believe that different ontological positions provide valuable insight that a single position cannot provide. We recognize that our recommendations posit some conflicting positions due to our choice to analyze fear appeals from both perspectives. However, both the critical realist and critical management analyses share the purpose of opening debates about and studies into the use of fear appeals in security practice.

We also recognize the prominent traditions that exist in behavioral InfoSec research (namely, positivist traditions). As such, we took a pragmatic stance that a critical review focused solely on social constructivist traditions may not have a strong effect on future fear appeal research. Thus, we felt it important to include a realist position to improve the chances that researchers will adopt and study the ideas we present. We hope that the dual perspectives we provide in this review open critical discussions from researchers who prefer either ontological position.

Admittedly, our paper—and research in general—adopts a frame that largely mimics a fear appeal. After reading enough motivation sections in academic work, one will surely come across messages about threats that researchers use to establish the need to study topics and remedies to the identified threats. One can see as much in behavioral InfoSec studies where researchers use insider and external threats to motivate studies. Motivating one's research is an academic tradition and identifying threats is an effective persuasive tactic that establishes the need to study a topic. Ironically, after writing this paper, we found that we unintentionally used fear appeals to set an agenda for the future study of fear appeals. In this paper, we discuss many ways that fear appeals can negatively influence insiders. We also question whether fear appeals are ethical and efficacious controls and whether they feed on researchers' fears of promoting unethical and ineffective controls. We found that writing the research motivation in a fear appeal style came naturally. For us, this realization further demonstrates the pervasiveness and invisibility of fear appeal logic in our lives. Despite the fear rhetoric we use to promote our analysis, we believe that the ideas presented herein are worth the time and effort to study.

5.2 Theoretical Contributions

Improving IS literature reviews is an important aspect of IS research (Tate, Furtmueller, & Evermann, 2015). Disciplines often reproduce ideologies through research studies, which traditional literature reviews may further reinforce (Alvesson & Sandberg, 2011; Maxwell, 2013). Thus, traditional literature reviews may only lead to incremental improvements in a discipline (Alvesson & Sandberg, 2011). Critical theories and methods provide novel means to analyze bodies of research to avoid the trap of small, incremental improvement (Wall et al., 2015). Existing critical review methods in IS research rely on Habermasian critical discourse analysis to analyze bodies of literature (Wall et al., 2015). However, many other useful theories, philosophies, and methods exist to critically analyze bodies of literature. We present two different ways to critically analyze academic research to provide direction for future study.

First, we draw on the philosophical positions of critical realism to analyze fear appeal research. Existing critical review methods in IS research are limited to constructivist philosophies (i.e., critical discourse analysis). Thus, we extend critical literature reviews into the domain of realist research. Second, we draw

on critical management studies other than Habermasian critical discourse analysis to provide constructivist critiques of fear appeals. Different constructivist theories and methods can lead to different implications (Stahl, 2008). Thus, one should use diverse critical methods to examine literature. By combining two critical philosophies, we provide a more holistic review that provides diverse directions for future research. Our review of fear appeal research answers calls for new forms of critical literature review in IS research (Wall et al., 2015).

5.2.1 Critical Realist Contributions

Our critical realist analysis points to several potential issues with the use of fear appeals in security settings and several important directions for future research. Existing research has followed certain traditions that have limited the study of fear appeals. Positivist research should focus on concepts that fear appeal research has excluded due to these prevalent research traditions; these concepts include: 1) the need to conduct more replication research to clarify empirical inconsistencies, 2) the need to understand fear control in security contexts, 3) the need to explore qualitative methods to identify new concepts that explain danger and fear control, 4) the need to include practical and management relevant concepts that will help practitioners design effective fear appeals, 5) the need to consider insider-centric outcome variables, and 6) the need to study the long-term effects and effectiveness of fear appeals. Our analysis provides useful areas of study that existing research does not address. Researching these areas may lead to improvements in the efficacy of fear appeals in practice.

By analyzing research from a critical realist position, we also identify several research traditions that may have led to these six exclusions (above). These restrictive research traditions include: 1) theory borrowing, 2) a preference for novel studies over replication studies, 3) overemphasis of protective behaviors, 4) a strong preference for quantitative research, 5) a fixation on management-centric perspectives, 6) a concern for theoretical parsimony, and 7) an overuse of cross-sectional research. None of these practices are inherently wrong. However, they can limit a research area if they dominate it. Our analysis of research traditions draws attention to common practices in behavioral information security research that relate in particular to the study of fear appeals. Researchers should be cognizant of these research traditions and be willing to break from them to identify new ways to view a topic. In doing so, the discipline will be less prone to ideological hegemony (Wall et al., 2015).

5.2.2 Critical Constructivist Contributions

Our critical management critiques also point to several issues with the use of fear appeals and identify several more directions for future research. We draw attention to the lack of interpretive and critical fear appeal research in security studies. More critical and interpretive research could explain the identities, beliefs, and values that fear appeals establish and identify the discursive closures they cause. The insights identified in the critical management analysis include: 1) the idea that fear appeals establish certain identities, beliefs, and values based on their underlying discursive logics; 2) the idea that fear appeals may create discursive closures that reify protective identities, beliefs, and values and exclude other viable positions; 3) the consideration that some discursive closures may be symbolic gestures to posture organizations as compliant with external regulations and norms to hide privacy-invasive behaviors; and 4) the consideration of vulnerable insiders who may be more susceptible to negative aspects of fear appeals. Existing studies mostly ignore these ideas due to the positivistic and managerial perspectives they adopt. Researching these other areas will provide a more holistic view of the effects of fear appeal use in the workplace.

Individually, each issue and insight in this paper may not call into question the effectiveness and ethicality of using fear appeals; however, in combination, they present reasonable doubt. If fear appeals are inconsistently effective or inefficacious for a large number of insiders and additionally cause negative effects for some or all insiders, then we need to question their utility. We do not contend that fear appeals are unethical or inherently wrong. However, we provide enough evidence to call for research to more carefully examine the efficacy of and the negative effects that result from the use of fear appeals in security control. We identify several theories and research questions to provide guidance for future research. Future research should examine these questions and consider other related questions and theories.

5.3 Alternatives to the Fear Appeal

Researchers often expect critical studies to identify solutions to issues identified during analysis (Myers & Klein, 2011). Thus, we now consider possible alternatives to fear appeals. Fear appeals are ultimately a form of persuasive appeal. Many persuasive appeals that do not rely as heavily on threat and fear to promote behavioral change exist. First, some call for reconstructing the fear appeal to downplay the role of threat messaging. Meta-analyses in extant research show that coping information increases behavioral change more than threat information (Ruiter et al., 2014). Thus, framing messages to increase employees' self-efficacy and response efficacy perceptions may be more beneficial than framing messages around threats. However, some studies also show that coping appraisals are not as effective when threat is low (Boss et al., 2015). Thus, researchers should continue to compare the relative strength that threat and coping messages exert on individuals' perceptions and behaviors. For example, researchers could design an experiment in which they provide a group of participants with a message that contains only a coping message and another group with a threat and coping message. Comparing the perceptions and behaviors of the participants across the two groups could provide evidence for or against the use of threat messaging in persuasive appeals.

Second, future research should consider other theories of persuasion that do not inherently rely on threats and fear. For example, the elaboration likelihood model (Petty & Cacioppo, 1986) describes how persuasive appeals influence individuals' attitudes and behaviors as they process the appeals through different cognitive routes. Though used less frequently, parts of the elaboration likelihood model suit behavioral InfoSec research (Johnston & Warkentin, 2010b; Puhakainen & Siponen, 2010). More deeply considering different persuasion theories could lead to managerial appeals that influence behavior but do not emphasize threats and fear. Similarly, persuasive appeals that rely on positive emotion, such as hope, empathy, and humor, may also effectively change behavior (Hastings et al., 2004).

Third, some security-related fear appeal studies have examined social influence (Herath & Rao, 2009; Johnston & Warkentin, 2010a). These studies have found that social influence strongly predicts secure behavioral intentions. Thus, developing a workplace environment and culture where insiders can develop strong security norms and values and support one another in security efforts may be a "friendlier" form of security control.

Fourth, security controls that grant insiders influence over their security behaviors, security policy, and security controls may improve security behavior. When organizations permit insiders to participate in developing information security controls, insiders demonstrate greater buy-in to security efforts (Spears & Barki, 2010). Additionally, according to self-determination theory (Ryan & Deci, 1985, 2000), when organizations permit individuals to determine their actions, they are likely to experience intrinsic motivation that leads to better outcomes (Ryan & Deci, 2000). Conversely, when organizations limit individuals' actions, they may react negatively toward control efforts (Posey et al., 2011; Wall et al., 2013).

Finally, we note that the four previous recommendations still promote protective identities, beliefs, and values that are likely to reify perceptions that organizations possess inalienable rights to own and use consumer information. Organizations should consider opening debates about information ownership and use in organizations to allow different beliefs and values to permeate organizational discourse. Enough concern over information ownership exists to warrant open internal discussions. The creation of new privacy protecting technologies, such as the blockchain, may leave organizations scrambling to cope with these potentially disruptive technologies if they have been unwilling to open discourse on topics of information ownership and use. Organizations may find it pertinent to remedy discursive closures caused by security-related fear appeals and other security controls to prepare for these developing technologies.

5.4 Management Implications

Organizations call on managers to establish and maintain control in organizations. This responsibility places managers in a position of power. Managers should recognize the discursive power they possess when they use fear appeals and other security controls. Our analysis provides insight into how fear appeals can affect discursive practice in organizations. Managers that desire to create a democratic environment can use the insights herein to minimize the likelihood of creating discursive closures. Namely, managers should consider opening debates about the ownership and use of information since security controls are likely to naturalize organizations' control over information. Our analysis also points to several vulnerable populations that managers should consider when designing security controls. Managers should avoid controls that exploit at-risk populations. Depending on a fear appeal's audience,

managers should consider altering the degree to which it induces fear. Managers should also carefully monitor the outcomes of fear appeals. To the extent that they can clearly identify some of the negative issues presented herein, managers can adapt fear appeals or adopt different security controls as outlined in the previous section.

6 Conclusion

Fear appeal studies in behavioral information security research are increasingly common. Many studies point to the usefulness of fear appeals as a form of security control in organizations. Individually, each fear appeal study shows that fear appeals affect insiders' in ways that promote secure behavior. However, some studies also point to small limitations in the use of fear appeals, which raises a question as to fear appeals' effectiveness. We review the fear appeal literature to identify themes across these studies that warrant future investigation. Through conducting a critical realist critique of the literature, we show that existing positivist research lacks important concepts, such as fear control responses, that limit current perspectives on fear appeal effectiveness. We provide directions for future positivist research to further explore and improve the effectiveness of fear appeals in different contexts.

Through a critical constructivist critique of existing research, we also note that fear appeal studies lack understanding about the effects that fear appeals exert on insiders. Fear appeals may not be ethical to use in some situations. Drawing on critical management studies, we show that fear appeals may limit the identities and values that insiders adopt in security settings and the associated implications. We provide important directions for researchers to study fear appeals from interpretive and critical perspectives. Existing fear appeal research is highly positivistic in nature. Studies of fear appeals from interpretive and critical perspectives will provide a more holistic viewpoint on the use of fear appeals in the workplace. In combination, our realist and constructivist critiques suggest that fear appeals may not be an effective nor appropriate form of control in the workplace. Researchers should study the directions for future research to determine and improve the effectiveness and ethical use of fear appeals.

Finally, our review and analysis of fear appeal research contributes to research on critical literature reviews. Critical literature reviews draw attention to hidden ideologies in research disciplines that potentially limit such disciplines. Thus, we need to improve these methods to open research discourse. In IS research, critical literature review methods are limited to Habermasian critical discourse analysis. By adopting critical realism and critical management philosophies, we point to different ways to structure a critical literature review. We show that critical literature reviews can adopt critical realist and critical constructivist positions to provide meaningful insight and research direction. By combining the two philosophical positions, we also provide a more holistic review than could be achieved by traditional review methods or by constructivist methods alone. Researchers should continue to improve critical literature review methods.

References

Al-Khouri, A. M. (2012). Data ownership: Who owns “my data”? *International Journal of Management & Information Technology, 2*(1), 1-8.

Alvesson, M., & Sandberg, J. (2011). Generating research questions through problematization. *Academy of Management Review, 36*(2), 247-271.

Baskerville, R. L., & Myers, M. D. (2002). Information systems as a reference discipline. *MIS Quarterly, 26*(1), 1-14.

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

Carrier, L. M., & Prashler, H. (1995). Attentional limits in memory retrieval. *Journal of Experimental Psychology: Learning Memory and Cognition, 21*(5), 1339-1348.

Christian, J. S., & Ellis, A. P. J. (2014). The crucial role of turnover intentions in transforming moral disengagement into deviant behavior at work. *Journal of Business Ethics, 119*(2), 193-208.

Corbin, J., & Strauss, A. (1990). Grounded theory method: Procedures, canons, and evaluative criteria. *Qualitative Sociology, 13*(1), 3-21.

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.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(2), 285-318.

Das, E. H. H. J., de Wit, J. B. F., & Stroebe, W. (2003). Fear appeals motivate acceptance of action recommendations: Evidence for a positive bias in the processing of persuasive messages. *Personality and Social Psychology Bulletin, 29*(5), 650-664.

Deetz, S. (2003). Disciplinary power, conflict suppression and human resources management. In M. Alvesson & H. Willmott (Eds.), *Studying Management Critically* (pp. 23-45). Los Angeles, CA: Sage.

Dennis, A. R. (2001). Relevance in information systems research. *Communications of the AIS, 6*(1), 40-42.

Dillard, J. P., Li, R., Meczkowski, E., Yang, C., & Shen, L. (2016). Fear responses to threat appeals: Functional form, methodological considerations, and correspondence between static and dynamic data. *Communication Research*.

Eisenhardt, K. M. (1985). Control: Organizational and economic approaches. *Management Science, 31*(2), 134-149.

Fida, R., Paciello, M., Tramontano, C., Fontaine, R. G., Barbaranelli, C., & Farnese, M. L. (2015). An integrative approach to understanding counterproductive work behavior: The roles of stressors, negative emotions, and moral disengagement. *Journal of Business Ethics, 130*(1), 131-144.

Foucault, M. (1977). *Discipline and punishment: The birth of the prison* (A. Sheridan, trans.). New York: Vintage Books.

Glassner, B. (2009). *The culture of fear: Why Americans are afraid of the wrong things* (tenth anniversary ed.). New York, NY: Basic Books.

Habermas, J. (1979). *Communication and the evolution of society*. Boston, MA: Beacon Press.

Habermas, J. (1984). *The theory of communicative action*. Boston, MA: Beacon Press.

Hastings, G., Stead, M., & Webb, J. (2004). Fear appeals in social marketing: Strategic and ethical reasons for concern. *Psychology & Marketing, 21*(11), 961-986.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal*, *24*(1), 61-84.

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

Hogan, M., & Shepherd, T. (2015). Information ownership and materiality in an age of big data surveillance. *Journal of Information Policy, 5*, 6-31.

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

Johnston, A. C., & Warkentin, M. (2010b). The influence of perceived source credibility on end user attitudes and intentions to comply with recommended IT actions. *Journal of Organizational and End User Computing, 22*(3), 1-21.

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

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*, 263-291.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23*(1), 67-94.

Lee, A. S. (1989). A scientific methodology for MIS case studies. *MIS Quarterly, 13*(1), 33-50.

Lehman, D. W., & Ramanujam, R. (2009). Selectivity in organizational rule violations. *Academy of Management Review, 34*(4), 643-657.

Leventhal, H. (1971). Fear appeals and persuasion: The differentiation of a motivational construct. *American Journal of Public Health, 61*(6), 1208-1224.

March, J. G., & Simon, H. A. (1958). *Organizations*. New York, NY: Wiley.

Maxwell, J. A. (2013). *Qualitative research design: An interactive approach* (3rd Ed.). Los Angeles, CA: Sage.

Mingers, J., Mutch, A., & Willcocks, L. (2013). Critical realism in information systems research. *MIS Quarterly, 37*(3), 795-802.

Myers, M. D., & Klein, H. K. (2011). A set of principles for conducting critical research in information systems. *MIS Quarterly, 35*(1), 17-36.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Ouchi, W. G. (1977). The relationship between organizational structure and organizational control. *Administrative Science Quarterly, 22*(1), 95-113.

Peters, G.-J. Y., Ruiter, R. A. C., & Kok, G. (2012). Threatening communication: A critical re-analysis and a revised metaanalytic test of fear appeal theory. *Health Psychology Review, 7*(1), S8-S31.

Petty, R. E., & Cacioppo, J. T. (1986). *The elaboration likelihood model of persuasion*. New York, NY: Academic Press.

Posey, C., Bennett, R. J., Roberts, T. L., & Lowry, P. B. (2011). When computer monitoring backfires: Privacy invasions and organizational injustice as precursors to computer abuse. *Journal of Information Systems Security, 7*(1), 24-47.

Posey, C., Roberts, T. L., & Lowry, P. B. (2016). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, 37(4), 1189-1210.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51*(5), 551-567.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly, 34*(4), 757-778.

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

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In B. L. Cacioppo & L. L. Petty (Eds.), *Social psychology: A source book* (pp. 153-176). London: Guilford Press.

Rotham, A. J., Salovey, P., Antone, C., Keough, K., & Martin, C. D. (1993). The influence of message framing on intentions to perform health behaviors. *Journal of Experimental Social Psychology, 29*, 408-433.

Ruiter, R. A. C., Kessels, L. T. E., Peters, G.-J. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology, 49*(2), 63-70.

Ryan, R. M., & Deci, E. L. (1985). *Intrinsic motivation and self-determination in human behavior*. New York, NY: Plenum Press.

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

Siponen, M. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security: Implications for research and practice. *Information Management & Computer Security, 8*(5), 197-209.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503-522.

Stahl, B. C. (2008). *Information systems: Critical perspectives*. London: Routledge.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: A critical evaluation. *Information Systems Journal, 22*(1), 77-94.

Tate, M., Furtmueller, E., & Evermann, J. (2015). Introduction to the special issue: The literature review in information systems. *Communications of the AIS, 37*, 103-111.

Thoresen, C. J., Kaplan, S. A., Barsky, A. P., Warren, C. R., & de Chermont, K. (2003). The affective underpinnings of job perceptions and attitudes: A meta-analytic review and integration. *Psychological Bulletin, 129*(6), 914-945.

Van't Riet, J., Cox, A., Cox, D., Zimet, G. D., De Bruijn, G. J., Van den Putte, B., de Vries, Werrij, M. Q., & Ruiter, R. A. (2016). Does perceived risk influence the effects of message framing? Revisiting the link between prospect theory and message framing. *Health Psychology Review, 10*(4), 447-459.

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from Electroencephalography (EEG). *Journal of the Association for Information Systems, 15*(10), 679-722.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*, 190-198.

Wall, J. D., Lowry, P. B., & Barlow, J. B. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems, 17*(1), 39-76.

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy and Security, 9*(4), 52-79.

Wall, J. D., Stahl, B. C., & Salam, A. F. (2015). Critical discourse analysis as a review methodology: An empirical example. *Communications of the Association for Information Systems, 37*, 257-285.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*, 101-105.

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

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs, 59*, 329-349.

Wolf, J. B. (2007). Is breast really best? Risk and total motherhood in the national breastfeeding awareness campaign. *Journal of Health Politics, Policy and Law, 32*(4), 595-636.

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

Wright, T. A., & Cropanzano, R. (1998). Emotional exhaustion as a predictor of job performance and voluntary turnover. *Journal of Applied Psychology, 83*(3), 486-493.

Xue, Y., Liang, H., & Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research, 22*(2), 400-414.

Yin, R. K. (2002). *Case study research: Design and methods* (3rd ed.). Thousand Oaks, CA: Sage.

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). *Decentralizing privacy: Using blockchain to protect personal data.* In *Proceedings of the IEEE Security and Privacy Workshops* (pp. 180-184).

About the Authors

Jeffrey D. Wall is an Assistant Professor in the School of Business and Economics at Michigan Technological University. His research interests include individual and organizational deviance and artificial intelligence. His research examines information security and privacy behaviors of employees in organizations. He also studies organizational behaviors related to the use and misuse of information assets. His research has appeared in the *Journal of the Association for Information Systems*, *Communications of the Association for Information Systems*, the *Journal of Information Privacy and Security*, the *Journal of Global Information Technology Management*, and the *International Journal of Organizational and Collective Intelligence*.

Mari W. Buche is an Associate Professor of Management Information Systems at Michigan Technological University (USA). She recently served as the inaugural Graduate Program Director for Data Sciences. She investigates issues related to the impact of technology change on information systems/technology employees within a business context. Her work has been published in the *Communications of the Association for Information Systems, Information Technology and Management Journal, Journal of Information Systems Education, International Journal of Networking and Virtual Organisations, Mid-America Journal of Business*, and numerous conference proceedings.