Journal of the Association for Information Systems

Research Paper ISSN: 1536-9323

Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination

Merrill Warkentin
Department of Management & Information Systems
Mississippi State University
m.warkentin@msstate.edu

Eric Walden
Data Science Programs
Texas Tech University
eric@ericwalden.net

Allen C. Johnston
Department of Management, Information Systems
University of Alabama at Birmingham
ajohnston@uab.edu

Detmar William Straub
MIS, the Fox School, Temple University
MIS, Korea University Business School
straubdetmar@gmail.com

Abstract:

Information security management programs have long included “fear appeals”, managerial communiqués designed to promote secure behaviors among organizational insiders. However, recent research has found a conflict between the predictions of contemporary fear appeal theory for how we expect individuals to experience fear appeals and what actually occurs in IS security situations. Using the opportunity presented by neuroimaging tools to examine cognitive and affective reactions to fear appeals, we take a comparative look at the contentions of fear appeal theory and the realities of what insiders experience neurologically when exposed to ecologically relevant IS security fear appeals. Our fMRI results suggest that fear appeals elicit threat and threat response assessments, which partially supports fear appeal theory but does not support the presence of an actual fear response. Furthermore, appraisals of recommended threat responses had a stronger impact on intentions to enact security behaviors than appraisals of the threat itself, which suggests that a focus on threats might be misplaced. Instead, focusing on ways to make the responses to the threats more appealing to users might work better. These controversial findings suggest future research that should explore how fear appeals play out in IS security and in what ways.

Keywords: IS Security, Neural Correlates, Fear Appeal Theory, Affect, Cognition, Threat, Threat Response, Self-efficacy.

Ting-Peng Liang was the accepting senior editor. This article was submitted on November 13, 2013 and went through 3 revisions.

1 Introduction

Contemporary organizations increasingly rely on the extensive use of information systems, systems that one must maintain and secure from numerous threats. Ironically, extensive research has pointed to the organizational insider, typically the employee, as the primary threat to the security of these very resources (Im & Baskerville, 2005; Stanton, Stam, Mastrangelo, & Jolton, 2005; Warkentin & Willison, 2009; Willison & Warkentin, 2013). Recent survey results (PWC, 2015) show that employees remain the most cited perpetrators of security incidents and that their crimes tend to be more costly to their firms than those that external sources commit. Furthermore, the results show that current employees and service providers were responsible for over 50 percent of reported incidents (PWC, 2015). Respondents in another recent survey indicated that carelessness or lack of awareness caused 38 percent of insider security incidents (Ernst & Young, 2014). An FBI report suggests that up to 20 percent of total company losses comes from non-malicious insiders (Richardson, 2011). These figures underscore the perennial mandate of decreasing the risk of negligent insiders in organizations (Guo, Yuan, Archer, & Connelly, 2011; Willison & Warkentin, 2013). In another study, surveyed organizations attributed 40 percent of data breaches to negligent employees (Ponemon Institute, 2012a; Wall, 2011). The recent dramatic rise in personal mobile devices in the workplace ("bring your own device" or BYOD practices (Lee, Crossler, & Warkentin, 2013)) and third party applications have introduced even more potential vectors for data leakage from employee carelessness and noncompliance (Ponemon Institute, 2012b).

For one, insider threats remain prominent because insiders often ignore their organizations' cybersecurity policies and procedures. Importantly, training, awareness, and leadership play important roles in supporting and reinforcing an organization's IS security policies (Puhakainen & Siponen, 2010), as do privacy and security values in the overall organizational culture (Van Niekerk & Von Solms, 2010).

Persuasive communications in the form of fear appeals also often support IS security policies (Johnston & Warkentin, 2010). Fear appeals are persuasive messages that highlight a threat to elicit a fearful emotional state that then motivates a subsequent behavioral response (which the message also recommends) (Witte, 1992). Being a primitive, natural state with which nearly all human beings resonate, fear derives from stimuli that seek to motivate changes in attitudes toward actions that facilitate positive results. These stimuli follow a prescribed course of action, especially protective behaviors. By exploiting the basic human emotions of fear and self-preservation, researchers believe that an effective fear appeal effectively articulates a threat while simultaneously providing guidance and support for implementing the recommended response for its amelioration.

When applied appropriately, fear appeals in many settings have proven to effectively facilitate behavioral change (Ruiter, Kessels, Peters, & Kok, 2014). In the health communication literature, for instance, threats to one's health or wellbeing have long been the catalyst for behavioral change (e.g., anti-smoking, anti-drug use, or seat belt safety campaigns). Examples of fear appeals in the health communication literature include public service announcements for HIV and AIDS awareness (Casey, 1995), drug abuse (Dillard, Plotnick, Godbold, Freimuth, & Edgar, 2006), drinking and driving, and skin cancer (Stephenson, 1993). In their study involving female college students, Fry and Prentice-Dunn (2005) found that women provided with coping information to detect and avert breast cancer were less likely to engage in maladaptive behavior rather than the recommended response. Others have also applied fear appeals to other fields. Hovland, Janis, and Kelly (1953) describe using fear appeals by government officials to summon support for national defense initiatives by underlining the dangers associated with being unprepared. We can find another example in the U.S. Office of National Drug Control Policy's using fear appeals in television advertisements to raise awareness of drug use among America's youth (Dejong & Wallack, 1999).

Studies also show, however, that fear appeals are not always effective across all audiences (Johnston, Warkentin, & Siponen, 2015), which is problematic in that for fear appeals to be used effectively, their influence needs to be predictable and aligned with the message's goals. The IS field and, in particular, scholars studying IS security fear appeals, who have struggled to understand and predict insider responses to policy-mandated directives delivered through fear appeals, currently face this challenge. In fact, applications of leading theories have resulted in mixed results and inconsistent outcomes (Johnston et al., 2015). The most recent models for predicting fear appeal responses include fear as a prominent affective component of how individuals process fear appeals. However, in the IS security literature, the role of fear is unclear, as is whether the most recent models are able to accurately predict responses to IS security fear appeals (Johnston et al., 2015).

Most individuals clearly experience the raw effect of fear (or fright) when someone points a gun to their head, but can we expect a similar affective reaction to the knowledge that identity thieves are targeting our computers? Similarly, when someone sees their house on fire, we would expect an affective response, but is that analogous to the response that occurs when one receives news that they may lose computer data? Given this background, how are IS security fear appeals perceived and experienced, and, as contemporary fear appeal theory espouses, are we truly experiencing fear as we understand it? These are the questions that drive this study and, by answering them, we have an opportunity to improve on fear appeal usage in IS security. In summary, the questions that motivated this study are: 1) “How are fear appeals experienced and perceived in the IS security context?”, and 2) “Are we truly experiencing fear as we understand it from contemporary fear appeal theory?”.

A limited body of rigorous studies examining the cognitive and affective responses elicited by fear appeals complicates our pursuit of these questions (Ruiter et al., 2014). The IS literature suffers from a similar limitation in that most IS studies involving fear appeals have constraints due to their scientific approach (i.e., most rely on self-reported surveys). The self-reported instruments may be well suited for studies of protection motivation, but we argue that they are not as well suited for gauging or exploring the neurological cognitive and affective responses theorized to be associated with fear appeal exposure. Subsequently, to explore these important gaps in our understanding of how individuals perceive IS security fear appeals, we use tools from the emerging neuroIS field. NeuroIS is the applied use of cognitive neurophysiological tools to study IS phenomena (Dimoka et al., 2012) and an evolving means by which to shed light on contentious phenomenological understandings.

Through an experimental design involving functional magnetic resonance imaging (fMRI), we studied the neural activities associated with the cognitive and affective reactions to fear appeals used for promoting secure behaviors. The results of this study demonstrate that, though articulated threats to IS security do cause cognitive responses consistent with fear appeal theory, they do not significantly determine protective intentions and do not elicit a sense of fear in the way most theories would lead one to expect. Rather, we found that the threatened individual’s efficacy to execute a recommended response to the threats motivates protective behavior. These findings have significant implications. IS security researchers should avoid relying primarily on fear appeal models deploying IS security-focused messages intended to scare users.

2 Theoretical Framework and Hypotheses

To understand how experience of fear appeals in IS security may differ from what fear appeal theory espouses, we need to first understand how fear appeal theory has progressed and where it stands today. In reviewing the fear appeal research, we found four primary theories that ground the preponderance of studies in this area (Roskos-Ewoldsen, Yu, & Rhodes, 2004; Witte, 1992). Hovland, Janis, and Kelly (1953) introduced the earliest such theory: the “fear-as-acquired drive model” (Hovland et al., 1953; Janis & Feshbach, 1953). This theory, which Janis (1967) later modified, describes an inverted U-shape relationship between motivation and fear during which an individual is motivated to take action to alleviate a threat only if a sufficient level of fear is present (Janis, 1967). Scholars initially referred to this action to address the threat as an “adaptive outcome” (and, later, as a “threat response”).

Janis (1967) further explained that, if too much fear is present, the resultant behaviors are oriented toward alleviating the sense of fear rather than addressing the danger itself directly. Researchers refer to this reaction as “maladaptive.” Maladaptive responses serve to neutralize fear by rejecting the fear appeal message or its source credibility (“he doesn’t know what he is talking about”), rejecting threat susceptibility (“it won’t happen to me”), rejecting self-efficacy (“I can’t do it”), or rejecting the response (“it won’t work”). McGuire (1968, 1969) posited a similar theory in which he also describes an inverted U-shaped relationship between fear and behavior. He argued that, when fear is a driving factor, individuals take actions consistent with the fear appeal’s recommended response to alleviate the threat. However, when fear acts as a cue, individuals often prefer previous behaviors that they use to successfully alleviate the fear.

Other scholars (Beck & Frankel, 1981; Rogers, 1983; Sutton, 1982) have since dismissed these early drive models of fear appeals and behavioral change (Janis, 1967; McGuire, 1968, 1969) because the former never fully supported a direct relationship between drive and behavioral change and because scholars found that arousal, as opposed to the reduction of arousal, influenced behavior (Mewborn & Rogers, 1979). In place of the drive models, Leventhal introduced the parallel response model, which distinguishes *affective* responses to a fear appeal from *cognitive* responses (Leventhal, 1970, 1971). The parallel response model asseverates that, when emotions motivate a response to a fear appeal, one is engaging in a fear control process, which is a maladaptive response. However, when cognitions of a threat motivate a response to it, one is engaging in a danger-control process—an adaptive response.

Rogers' (1975) protection motivation theory (PMT) further advanced Leventhal's (1970, 1971) work by expounding on the danger-control process and suggesting that a fear appeal has three primary elements that an individual assesses when exposed to a fear appeal message: threat susceptibility, threat severity, and response efficacy. Later, Rogers (1983) identified self-efficacy as a fourth component of the danger control process. PMT posits that an individual, when exposed to a fear appeal, will first appraise the described threat's significance and severity. This is a threat appraisal. In circumstances where the fear appeal is successful in eliciting a perception of significant and serious threat, the individual will then consider the recommended response to alleviate the threat both in terms of the perceived efficacy of the response and the individual's ability to enact the response. This is a coping appraisal.

Finally, Witte (1992) examined the extant models involving fear appeals and concluded that a gap existed in describing interactions of the components of a fear appeal and the role of fear itself in persuasive arguments. Witte combined Leventhal's (1970, 1971) parallel process model and Rogers' (1975) protection motivation theory to better explain how fear appeals influence or do not influence the behaviors of their audience (see Figure 1).

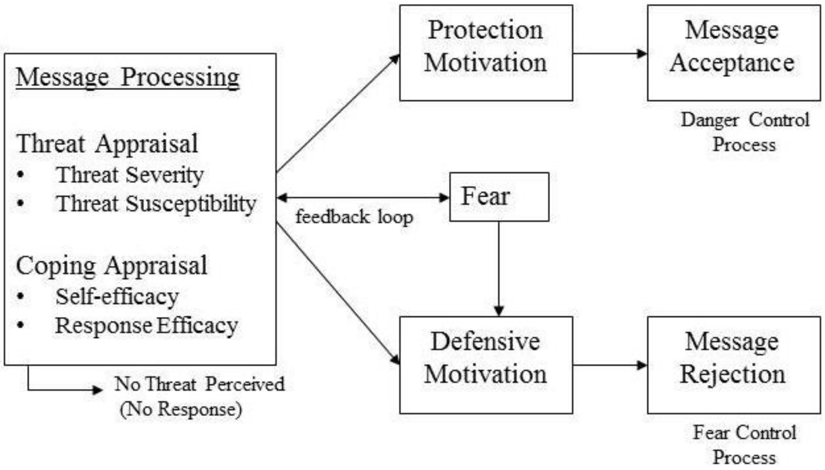


Figure 1. The Extended Parallel Processing Model (Witte, 1992)

The extended parallel processing model (EPPM) maintains that, when one attempts to control fear processes, one is defensively motivated, which leads to message rejection. In this state, cognitions of the threat and the efficacy of the recommended response are minimal and the fear emotion is prominent. Alternatively, when individuals perceive that they can effectively and feasibly avert a threat, thoughts of the threat and efficacy will directly influence message acceptance. However, EPPM suggests that, in this state, individuals may recognize their fear emotion and may then cognitively alter their perceptions of a threat's severity. In other words, persons with a high perception of efficacy may notice physiological symptoms associated with fear, such as sweating palms or a racing pulse, and consider these symptoms to mean that they perceive the threat to be greater than they originally thought. From reassessing the perceived threat, they will often change motivation for message acceptance.

2.1 Neuroscience Research into Fear

Society has long recognized fear's power; as Lovecraft (1945, p. 1) notes, it is mankind's "oldest and strongest emotion". Psychologists distinguish between primary and secondary emotions. Primary emotions are those we feel as an initial response to a stimulus, whereas secondary emotions (which the primary emotions often cause) appear afterwards. For example, when one feels threatened, the primary emotional response is fear, which may be followed by the secondary emotion of anger, which may lead one to take action in the classic fight or flight response. Darwin (1877) suggested that fear is probably one of the earliest feelings that infants experience. Indeed, fear has been the subject of exploration for all of written history. For instance, the Epic of Gilgamesh, largely considered the oldest known work of literature, explored the effects of the fear of death on human behavior over 4000 years ago. As such, one should not be surprised that some of the first fMRI work on emotions looked at fear. This research started by assessing fear conditioning (LaBar, Gatenby, Gore, LeDoux, & Phelps, 1998), which pairs a stimulus to be feared (e.g., electrical shock) with a neutral stimulus (e.g., a blue square shown on a screen). Though early work using PET scanners was inconclusive, fMRI showed a role for the amygdala in fear conditioning (LaBar et al., 1998). Research further confirmed that the amygdala is not only important for learning fear but also for representing fear (Phelps et al., 2001). The amygdala also seems to play a role in recognizing fear in others in that it shows increased activation when viewing fearful faces versus happy faces and when viewing more fearful faces versus less fearful faces (Phelps et al., 2001).

More recently, fMRI research has turned toward studying phobias, particularly spiders (Aue et al., 2015; Clemente et al., 2013; Zilverstand, Sorger, Sarkheil, & Goebel, 2015) and dentists (Hilbert, Evens, Maslowski, Wittchen, & Lueken, 2014; Scharmüller et al., 2014; Schienle, Scharmüller, Leutgeb, Schäfer, & Stark, 2013). These studies focus on interventions to reduce phobias. For example, researchers have instructed groups of dental phobic people either to classify the contents of a picture (focus on its content) or to evaluate whether the picture was pain relevant (focus on associations with pain). They found that when individuals considered the pain aspect of a picture, there was greater activation of their amygdala than when individuals thought about a picture’s content (Scharmüller et al., 2014). Fear conditioning remains the most widely studied area of fMRI work (Fullana et al., 2015). Although one can learn fear conditioning and apply it to extinguish fear, we focus on a different role for fear. We focus on conveying messages to individuals that introduce fear as a motivator and using fear in persuasive communications to encourage action. Fear is an uncomfortable affective state that leads organisms to take actions, and we investigate that motivating effect in this work.

In general, psychologists and neurologists will more likely work toward removing irrational fears. They would less likely be interested in removing irrational feelings of complacency, which is effectively what an IS fear appeal is designed to do. Thus, the extant literature using fMRI to study fear is generally in a very different vein. The notable exception is smoking, where psychologists do study fear appeals using fMRI (Dinh-Williams, Mendrek, Dumais, Bourque, & Potvin, 2014). Unfortunately, smoking is a chemical addiction and the dangers are widely known, so the findings are largely that smokers and non-smokers perceive fear appeals differently. Unfortunately, we do not have an analog to nicotine-addicted individuals in IT security fear appeals.

2.2 Research Hypotheses

As we describe in Section 2 and 2.1, the social psychology research community has firmly established the process for assessing fear appeals. Contemporary fear appeal theory provides two important assumptions about fear appeals. First, fear appeals must be personally relevant to their intended audience. Without personal relevance, any articulated threat will not be able to engender the level of perceived severity and susceptibility required for a response. Second, fear appeals must be able to elicit a sense of fear in their intended audience. Contemporary fear appeal theory positions fear as a leading predictor of how an individual will assess a fear appeal. The theory suggests that an individual will conduct threat and coping appraisals, which will subsequently influence and be influenced by fear of the threat.

In the health communication literature, which widely applies fear appeal theory, research findings have consistently upheld these assumptions, and researchers have long used threats to one’s health or wellbeing to create behavioral change (e.g., anti-smoking, anti-drug use, or seat belt safety campaigns). In their meta-analytical study of the health communication literature, Ruiter et al. (2014) found strong support for the conventions of fear appeal theory in explaining how individuals form behavioral responses when the context of the threat was one in which threat exposure was sufficient to generate fear, but was also controllable through the actions of the individual. In the IS security literature, however, researchers have not always found results concerning the warnings of threats to IS security to be consistent with fear appeal theory. For example, whereas some studies position the threat appraisal constructs (susceptibility and vulnerability) as having a direct effect on behavioral intentions (Crossler, 2010; Lee & Larsen, 2009; Woon, Tan, & Low, 2005), other studies model the threat appraisal constructs having both a direct effect on behavioral intentions and an interaction effect with the coping appraisal constructs (response efficacy, self-efficacy, and response cost) (Liang & Xue, 2009, 2010). Other studies model their adaptation of PMT as having no direct effect on behavioral intention but a direct effect on another variable such as omissive behavior (Workman, Bommer, & Straub, 2008), attitudes (Anderson & Agarwal, 2010; Herath & Rao, 2009), or coping appraisal (Johnston & Warkentin, 2010), which then has a direct effect on behavioral intention. Further, some studies include response costs as part of the coping appraisal analysis (Lee & Larsen, 2009; Liang & Xue, 2010), while others omit this factor (Anderson & Agarwal, 2010; Johnston & Warkentin, 2010). Not all studies have not shown the threat appraisal constructs of severity and vulnerability (or susceptibility) to influence information protection motivation (Crossler, 2010; Herath & Rao, 2009; Johnston & Warkentin, 2010; Woon, Tan, & Low, 2005).

We contend that this discrepancy results from violations of the two underlying assumptions of fear appeals (as we present above); namely, the non-personal nature of the threats and the subsequent absence of fear (Johnston et al., 2015). Threats to one's digital assets or intellectual property do not carry the same personal implications as threats to one's health. Further, threats of a non-personal nature are not likely to generate fear, which limits strong perceptions of threat. Threat and coping appraisals will still occur, but fear will not be present and, therefore, will not reinforce any derived threat or efficacy perceptions. We base this argumentation on inferences drawn from the inconsistent results found in the IS security literature (Johnston et al., 2015).

Building on this logic, we expect to see some consistencies and some discrepancies in terms of how individuals process fear appeals in the IS security context. One consistency we expect to see relates to the personal nature of threat appraisals, which one should not confuse with a threat's personal relevance, which describes the degree to which a fear appeal frames a threat as having particular significance. Even though we contend that IS security threats do not share the same personal relevance as context-specific threats (such as personal health), we expect that individuals will still appraise threats in a self-referential manner. That is to say, when presented with an articulated threat, fear appeal theory suggests that one will consider the threat relative to their own experience. Neuroscience calls this cognitive process *self-referential thinking* (Bhatt & Camerer, 2005). This process should effectively reveal the personal relevance; by assessing a threat from a self-referential perspective, the individual should envision its degree of personal relevance.

Neuroscience researchers have widely studied self-referential thinking in a variety of settings. A recent meta-analysis of self-referential thinking studies (Northoff et al., 2006) found that several cortical midline structures consistently activated more in self-referential thinking than in control conditions. The literature shows that these structures can be differentiated into three clusters in the frontal midline corresponding roughly to 1) the pre- and subgenual anterior cingulate cortex, 2) the supragenual anterior cingulate cortex, and 3) the medial parietal cortex (see Figure 2 in Northoff et al. (2006) reproduced below). Regardless of a threat's context, if one perceives that threat as a potential menace to one's self or one's environment, one will assess it relative one's self. Therefore, we hypothesize:

> **Threat appraisal hypothesis (H1):** When one appraises threat statements (exposure to a fear appeal's threat-related component), brain areas associated with self-referential thinking, including cortical midline structures, will be activated more than when one appraises a neutral statement.

We also expect to see consistency between the threat response coping appraisals established by fear appeal theory (in other contexts) and those appraisals of individuals when assessing fear appeals in the IS security context. Threat responses are, indeed, similar to the self-referencing manner in which one assesses threats. In an effort to assess the effectiveness of a response and the efficacy of their ability to enact the response, individuals will consider them relative to their personal goals and abilities. Therefore, we hypothesize:

> **Coping appraisal hypothesis (H2a)**: When one appraises coping statements (exposure to a fear appeal's recommended response component), brain areas associated with self-referential thinking, including cortical midline structures, will be activated more than when one appraises a neutral statement.

Fear appeal theory also suggests that engaging in a recommend threat response will reward insiders. That is to say, the threat response provides a reward by alleviating the negative fear state induced by the threat. The reward inherent in engaging in the response provides one with the motivation to engage in the response. Thus, insiders should be making value judgments when appraising a threat coping response regardless of the threat's personal or non-personal nature.

The area of the brain most often associative with reward is the nucleus accumbens (Dimoka, Pavlou, & Davis, 2011). Research has found the nucleus accumbens to be associated with monetary rewards (Matthews, Simmons, Lane, & Paulus, 2004), snacking (Lawrence, Hinton, Parkinson, & Lawrence, 2012), and cocaine use (Reid et al. 1997). If an individual appraises a response consistent with the expectations of fear appeal theory, the individual will consider the response relative to its rewards. We therefore hypothesize:

> **Coping appraisal hypothesis (H2b):** When one appraises coping statements (exposure to a fear appeal's recommended response component), brain areas associated with reward evaluation,

specifically the nucleus accumbens, will be activated more than when one appraises a neutral statement.

Where we expect to see a discrepancy between IS security fear-appeal assessments and the expectations set forth by fear appeal theory relates to fear responses. The area most often associated with fear is the amygdala. Research has shown amygdala activation to correlate with viewing frightened faces (Morris et al., 1996), experiencing negative responses during fear conditioning (Bechara et al., 1995; LaBar et al., 1998), and seeing spiders (Dilger et al., 2003; Larson et al., 2006). In addition, research has found that stimulating the amygdala raises corticosteroid levels by up to 400 percent (Rubin, Mandell, & Crandall, 1966). Corticosteroids are hormones that the adrenal glands release in response to stressors such as fear. As we state above, we contend that the non-personal nature of IS security threats makes them not likely to generate the emotion of fear. Threats to the IS security of an organization, to its data, and to its information systems do not convey the same level of threats to a person as threats to one's health, safety, or personal wellbeing. IS security threats are assessed relative to one's self but may lack personal relevance and, thereby, fail to stimulate threat perceptions or cause an emotional fear response (Johnston et al., 2015). Therefore, we hypothesize:

> **Fear elicitation hypothesis (H3):** When one appraises an IS security-related fear appeal, brain areas associated with fear, specifically the amygdala, will be activated no more than when one appraises a neutral statement.

3 Method

To explore our research questions, the evolving neuroIS field provides several neurocognitive tools by which to gain insight into the presence and role of fear in fear appeal assessment and into the elements of a fear appeal that most impact security-response intentions. Based on the insights that Riedl et al. (2010) and Dimoka et al. (2012) provide, we conducted a lab experiment and analyzed the responses of subjects through functional magnetic resonance imaging (fMRI) tools to observe and evaluate the reactions of insiders' neural structures to IS security-focused fear appeals and their cognitive and affective neural responses.

3.1 Research Design

We studied the reactions of insiders' neural structures to controlled stimuli commonly found in IS security-focused fear appeals via a within-subjects experimental design. A within-subjects design allows researchers to use each subject as the subject's own experimental control.

We designed stimuli to be ecologically relevant in the sense that we offered subjects the same sorts of fear appeals that insiders typically see in actual organizational environments. We designed these appeals to be framed as managerially created statements that describe a security threat and its aftermath. Please see Appendix A for examples of the language elements we used in these screens. An expert panel comprising six experienced individuals (two were IS security managers, two taught business communications, and two were scholars with experience in experimental design) reviewed each fear appeal and neutral statement. We asked the panel to evaluate the potential relevance of the appeals and the extent to which they differed from non-relevant neutral statements. Following the review, we edited and revised the appeals and neutral statements repeatedly until all experts were satisfied. A second panel of subject matter experts comprising six IT professionals from two organizations validated the appeals' content validity (realism), technical correctness, and consistency with the rhetorical situation.

Typical of most fMRI studies (Dimoka, 2012), we used student subjects from a business school subject pool in a large university in the southern US (N of subjects was 17). The average age was 22.5 years (min = 20, Max = 29, stdev = 2.48). Fourteen males and three females participated, and two subjects were left-handed. The subjects received course credit for participating. We asked each participant a series of questions before coming to the fMRI scanner about their age, sex, education attainment, and experience with computer technology.

Students constituted an appropriate sampling frame for two reasons. First, they are members of an organization that has information systems security policies requiring compliance; in this environment, known IS security threats exist, and, in this sense, they are trusted insiders. Beyond responsibility to the organization, students also have personally valuable information assets to protect and are subject to the same protection motivation factors as any other computer user. They can choose bad passwords, fail to back up data, or lose their portable drives. Thus, they represent the targeted population where there are real-world responses required on their part to address the damage from real threats. We crafted a set of threat responses and displayed them to our subjects as experimental stimuli. A panel of expert IS security managers scrutinized these recommended responses and validated that they represented realistic response recommendations found in organizations. Second, these subjects all studied business school courses, and, hence, the majority were planning on a business career in which they would face the same issues again. Finally, according to Gordon, Slade, and Schmitt (1986), student subjects are appropriate when real-world experience will not diminish the intensity of their responses to the stimuli. Thus, in our experimental setting, students represent perhaps a more robust sample for testing fear appeals because they have no jobs to lose as would real employees, which means that, because fear and other brain activations are more difficult to stimulate, our results are even more significant than results we might have generated using employees. Moreover, we observed the rigorous guidelines for student sampling frames that Compeau, Marcolin, Kelley, and Higgins (2012) provide and identified the parallel elements of the task and method used in our manipulation. Specifically, these factors are the fear appeal statements and the protection motivation factors that we identify in Table A1. Therefore, the brain activations we recorded represent more robust findings than would otherwise be the case.

A single trial of the experiment started with a jitter [1] fixation cross-displayed for a random amount of time between 0 and 1TR (2.5s). Following this jitter was a neutral statement about information technology for five seconds[2], a second jitter, and an IT threat statement for five seconds. Then, we asked subjects to indicate their agreement on a seven-point Likert scale with the statement, “If [THREAT] occurred, the consequences would be severe”. Subjects could take as much time to answer this question as they needed, but, on average, they took around two seconds. Next, we asked them to indicate their agreement with the questions following the format “[THREAT] is likely to occur”. After this, they were given another jitter, shown a response to the threat, followed by another jitter. We then asked them about how well they agreed with the statement “[RESPONSE] is effective for [THREAT]”. After this, we asked them about how well they agreed with agreement with the statement “[RESPONSE] is easy to do” and finally how well they agreed with the statement “I plan to engage in [RESPONSE]”.

Each of the neutral, threat, and response statements had the same number of words in a given trial. There were thirty different neutral, threat, and responses triplets. Table 1 shows the experimental procedure. We scanned participants’ brains continuously throughout the experiment.

Table 1. Experimental Procedure

Jitter (0-2.5s)	Neutral statement (5s)	Jitter (0-2.5s)	Threat statement (5s)	Threat severity measure (self-paced)	Threat susceptibility measure (self-paced)
Jitter (0-2.5s)	Response statement (5s)	Jitter (0-2.5s)	Response efficacy measure (self-paced)	Self-efficacy measure (self-paced)	Behavioral intention measure (self-paced)

We conducted the scans using a Siemens Skyra 3 tesla machine. Functional imaging had a repetition time of 2.5 seconds, an echo time of 30 milliseconds, and a flip angle of 90 degrees. Voxels were $3mm^3$ with 44 slices taken in the transverse plane in an interleaved fashion. The number of volumes taken depended on how fast subjects answered the evaluation questions and ranged from 818 (34:05 minutes) to 1284 (53:30 minutes). We also took high-resolution T1 images with a voxel resolution of .9375 mm X .9375 mm and a slice thickness of .9000mm. These images contained 192 slices in the sagittal plane.

We registered the functional images to the T1 images using FSL’s FLIRT (Jenkinson, Bannister, Brady, & Smith, 2002; Jenkinson & Smith, 2001) BBR algorithm (Greve & Fischl, 2009). We then registered the high-resolution images to the standard 2mm Montreal Neurological Institute 152 brain using FSL’s FNIRT (Andersson, Jenkinson, & Smith, 2007) using a warp resolution of 10mm and a 12 degree of freedom search. We corrected for motion using FSL’s MCFLIRT (Jenkinson et al., 2002). We spatially smoothed

[1] The TR is the time it takes to scan the entire brain. Jitter is simply a time interval between two stimuli. By adding jitter between 0 and 1TR, we ensured that the scan for the next stimuli started at a random spot relative to the scan for the previous stimuli. Doing so removes correlations with the timing of acquiring the scans. See Dale (1999) for a more complete discussion.

[2] This measure served as the within-subject control benchmark as is typical in neuroscience experiments.

images using a Gaussian kernel with a 5mm width. We applied high-pass filtering using a least-squares straight line fitting with normal kernel with a sigma of 50 seconds. We extracted non-brain matter data using BET (Smith, 2002).

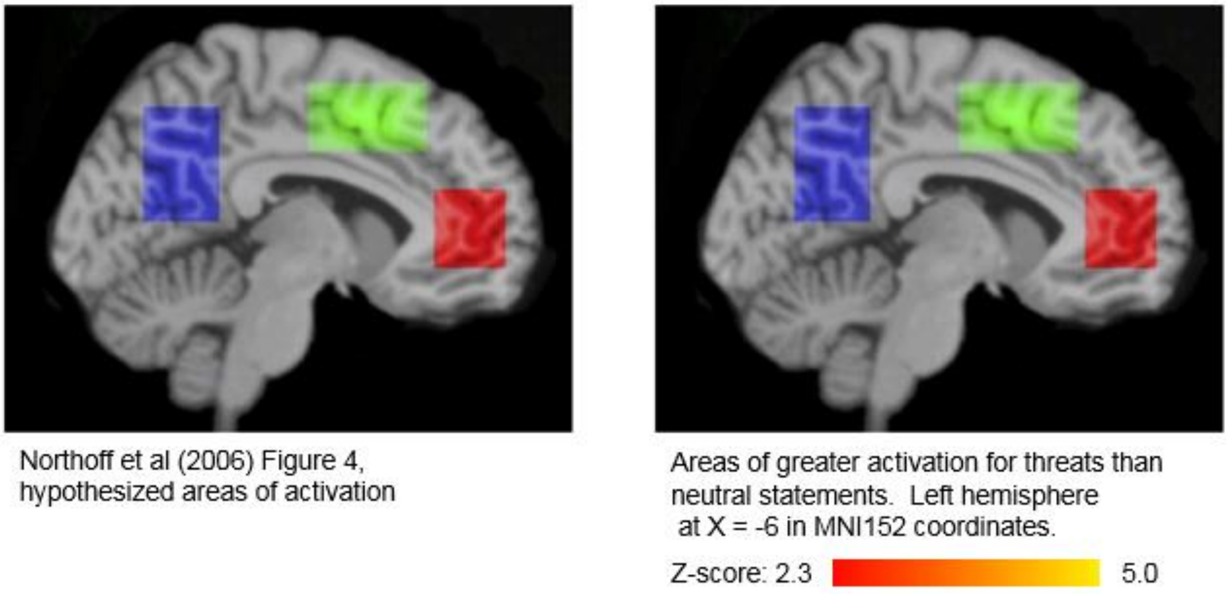
We used a generalized least squares model to fit the individual level data. We created five dummy variables equal to one for the time periods that corresponded to: 1) neutral statements, 2) security threats statements, 3) responses to threats statements, 4) fixation crosses during jitter, and 5) times subjects viewed and answered the evaluation questions. We then convolved these dummy variables with a gamma function with a lag of six seconds and a standard deviation of three seconds to approximate the hemodynamic response function (Woolrich, Jenkinson, Brady, & Smith, 2004). We added temporal derivatives to compensate for minor differences in the hemodynamic response function in different voxels.

4 Results

To test H1, we contrasted brain activation while people viewed neutral statements to brain activation while people read threat statements. In effect, we subtracted brain activation while someone read a statement from brain activation while someone read a threatening statement. In principle, this left the activation associated only with the threats, not the act of reading text. To test H2b, we contrasted activations when we presented the response statements to the activation when we presented the neutral statements, which, again, effectively removed the activation components associated with reading and left only those associated with evaluating responses.

4.1 Test of Threat Appraisal Hypothesis

With respect to H1, appraisals of IS security threats showed several areas of activation greater than neutral stimuli. The areas of neutral activation were the dorsolateral prefrontal cortex bilaterally, supragenual anterior cingulate cortex, pre- and subgenual anterior cingulate cortex, medial parietal cortex, the lingual gyrus bilaterally, the intracaalcarine gyrus bilaterally, the cuneous bilaterally, and the angular gyrus bilaterally. Interestingly, all three of the areas identified by Northoff et al. (2006) had activation, which Figure 2 shows. These findings support the threat appraisal hypothesis in that insiders engage in self-referential thought when viewing IS security threats and, thereby, assess the threat in a manner consistent with fear appeal theory.


Northoff et al (2006) Figure 4, hypothesized areas of activation

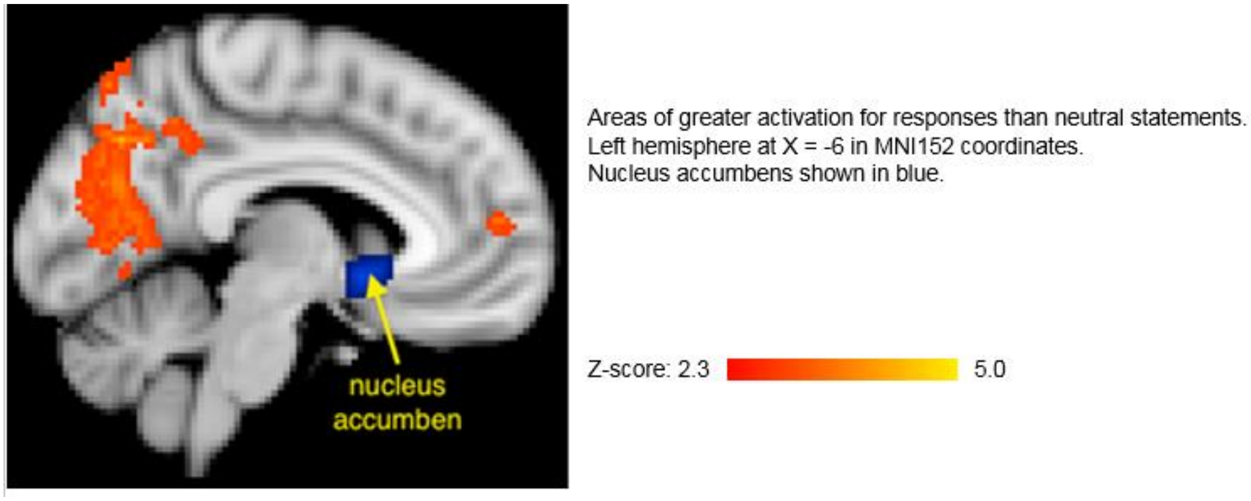
Areas of greater activation for threats than neutral statements. Left hemisphere at X = -6 in MNI152 coordinates.

Figure 2. Threat Appraisal Results

4.2 Test of Coping Appraisal Hypotheses

With respect to H2a, appraisals of threat responses revealed activation along the same midline structures that H1 hypothesized. This finding suggests that, when presented with threat responses, insiders engage in self-referential thinking, a reasonable reaction given that responses to threats are actions that the insiders must perform themselves.

We did not find support for H2b, which suggests that, when appraising coping statements, insiders evaluate the reward value of the recommended threat response). As Figure 3 shows, we found no clusters of activation in the nucleus accumbens, and, indeed, no single voxel survived thresholding. An ROI analysis would not change these results. Note that, compared to just reading statements about computers, being offered a response to an IS security threat did not engage the brain's reward centers, which suggests that individuals do not evaluate responses to IS security threats as rewards.



Areas of greater activation for responses than neutral statements.
Left hemisphere at X = -6 in MNI152 coordinates.
Nucleus accumbens shown in blue.

Figure 3. Coping Appraisal Results

From these results, we ascertain that coping appraisals of IS security threats do occur in a self-referencing manner consistent with fear appeal theory but do not elicit the sense of reward that we expected from thwarting security threats. Perhaps the non-personal nature of the threats inhibits a sense of reward from their amelioration, a consequence of violating one of the underlying assumptions of fear appeal theory.

4.3 Test of Fear Elicitation Hypothesis

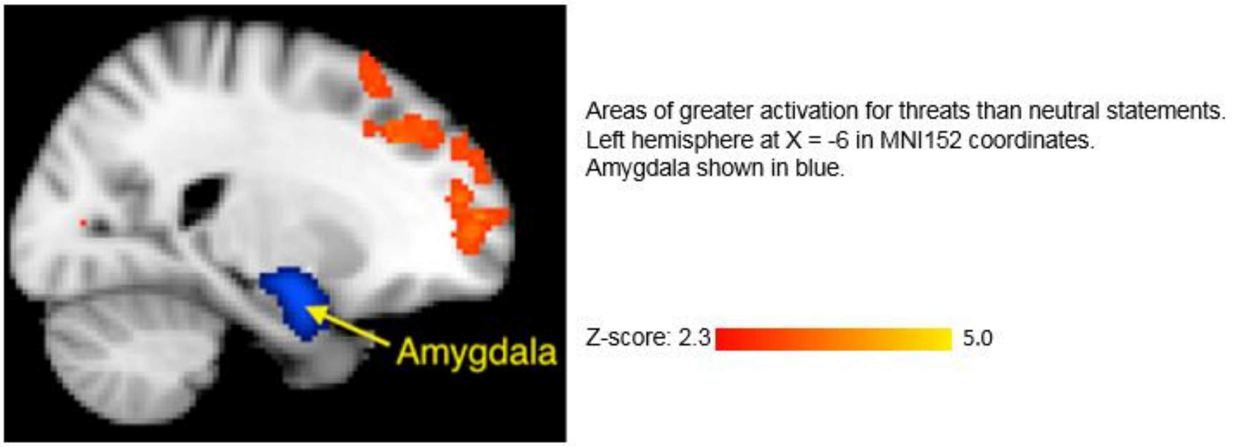
For H3, as expected, insiders showed no significant activation in the amygdala, which suggests that the emotion of fear was not invoked when they were exposed to the security threat statements[3] (see Figure 4). In fact, we found no clusters of activation in any limbic regions, which suggests that threats to IS security inspire little emotional consequence. Beyond regions implicated in the threat appraisal and fear hypotheses, we also saw greater activation in the inferior parietal region bilateral and the superior frontal regions bilaterally. Collectively, these areas suggest a network of visual attention, which is consistent with the idea that threats motivate more attention than neutral statements (Hopfinger, Buonocore, & Mangun, 2000). This outcome is also consistent with the finding that attention was motivated by the fact that the insiders knew they were going to be asked questions about the threats.

The reverse contrast (areas where the neutral statements produced greater activation than the threats) showed a small area of activation in the medial thalamic nucleus. Recently, research has shown this region to be activated subsequent to motor tasks (Klingner, Hasler, Brodoehl, Axer, & Witte, 2013; Tung et al., 2013). In all trials except for the first, we presented neutral statements after the motor task of answering

[3] For this study, we used whole brain, familywise error-corrected images so that we could examine all regions of the brain (even those not associated with hypotheses). In general, we performed a region of interest (ROI) analysis and looked only at the regions hypothesized. However, we did not need to in light of our results, so, in the interest of space, we offer this footnote. The advantage of the ROI analysis is greater statistical power to detect effects because of doing a familywise error correction over fewer voxels; thus, one can detect smaller clusters. However, in the amygdala, no voxels survived thresholding, so, if zero voxels were significant, there was no advantage of greater power. At the same time, we found activation in all three of the areas hypothesized for the self-referential thinking hypotheses, and increasing power through an ROI analysis would only make those results stronger.

evaluation questions; thus, we can reasonably believe that this activation is a symptom of switching from a motor state to an attention state.

In summary, during threat appraisal, evidence suggests that insiders engage in self-referential thinking—presumably to contemplate how the threat affects them, but no evidence suggests that the threat generates fear or, indeed, any emotional response at all. Individuals seem to perceive IS security threats more as facts that they need to address rather than as fear-inducing threats.



Areas of greater activation for threats than neutral statements.
Left hemisphere at X = -6 in MNI152 coordinates.
Amygdala shown in blue.

Figure 4. Fear Elicitation Results

4.4 Findings Regarding Threats and Responses

In addition to the hypothesized activations, we found other activations of interest. First, coping appraisals of the threat responses produced activation in the right cerebellum in a region called the crus I. Research has shown this area to be active when one processes actions that require multiple steps (Balsters, Whelan, Robertson, & Ramnani, 2013). In the context of threat responses, this activation makes sense because a response is ultimately a series of steps. Thus, coping appraisals seem to differ from threat appraisals in that they require one to consider actions. Also, we note the responses lacked the activation in the superior frontal lobe that was present when viewing threats, which suggests that threats involve more processing of uncertainty than do responses. Both the greater activation in the cerebellum for responses and the greater activation in the superior frontal lobe for threats were statistically significant in the contrast of threats and responses.

4.5 Behavioral Intention

Another interesting finding concerns the relevant roles of each of the fear appeal elements on behavioral intentions to engage in recommended threat response behavior. A regression analysis of the survey data reveals that self-efficacy had about 40 percent more impact on behavioral intentions than all of the other measures put together (see Table 2). Self-efficacy and response efficacy were the two highest determinants of behavioral intention in standardized beta coefficient value and had a total effect of 0.75, whereas the threat measures had a total effect of 0.2. In sum, appraisals of threat responses (coping appraisals) stimulated about four times the effect on behavioral intention as appraisals of the threat itself (threat appraisals). For this reason, fear appeals deployed in an IS security context should focus on articulating the efficacy of a threat response and in building up the perceived self-efficacy of the person charged with its implementation than on the threat, its severity, and potential likelihood.

Table 2. Determinants of Behavioral Intention

	Susceptibility	Severity	Self-efficacy	Response efficacy	Intercept
Coefficient	0.026	0.082	0.566	0.185	-0.028
T-score	-0.763	2.067	17.658	4.901	-0.098
Prob t (2 sided)	0.445	0.039	< 0.001	< 0.001	0.922

5 Discussion

The questions that motivated this study were: 1) “How are fear appeals experienced and perceived in the IS security context?” and 2) “Are we truly experiencing fear as we understand it from contemporary fear appeal theory?”. Fear appeals have been used for decades as an essential form of persuasive communications to engender compliance among insiders with IS security policies. We show, however, that IS security fear appeals are not as effective as those in other fields, such as healthcare or public service campaigns (Bélanger & Crossler, 2011; Crossler et al., 2013; Herath & Rao, 2009; Johnston & Warkentin, 2010; Johnston et al., 2015). This finding may indicate a need to reassess the orthodox presumptions in our research community: do the expectations of fear appeal response put forth by contemporary fear appeal theory misalign with how they are actually experienced in IS security situations (Johnston et al., 2015)?

Our results suggest that individuals do attend more to both threats and threat responses than to neutral statements and that their assessments of threat and threat responses mostly conform with fear appeal theory. Individuals seem to engage in self-referential thinking in assessing both threat and threat responses. However, they do not seem to experience fear or any type of emotional reaction to threats, nor do they seem to view threat responses as rewarding. Moreover, they do appear to be more uncertain when assessing threats than when assessing threat responses, which conforms with the stance that threats are probabilistic outcomes in which insiders are not likely fully aware of the threats’ details or ramifications. Finally, individuals seem to engage more in planning action when viewing responses, which make sense in that responses are actions the individual must take.

Our results also suggest that, from a neurological perspective, threat responses are as interesting and complex as the threats themselves and, from the standpoint of behavioral intentions, responses are much more important. This leads one to conclude that the more important component of a fear appeal—the threat response—has received insufficient attention in the literature, implying that future research and practice should focus more on responses to threats than to the threats themselves. This finding, along with the absence of an emotional fear response, helps explain how IS security fear appeals may actually operate. This finding appears to be at variance with contemporary fear appeal theory predictions. In the future, IS security scholars should recognize this contradictory evidence and show caution when studying fear appeals, applying fear appeal theory, or using fear appeals as part of a study involving persuasive communications.

Finally, from our results, what seems to be conspicuously missing is the motivation for compliant IS security behaviors. The fMRI results suggest that threats may not engender strong fear and, thus, the desired motivation to engage in protective responses to the threats. Threat responses also do not provide a reward to drive behavior. At the same time, subjects indicated they would subsequently engage in protective behaviors, so something clearly must be driving their behavioral intention. Self-efficacy was the largest behavioral predictor in our data. To the degree that self-efficacy makes a behavior easier, this finding suggests that the motivation for computer users may have included effort minimization. Though users will undoubtedly feel better knowing that their data is secure, they may pursue many IS security behaviors for the simple functional benefits in the same routine way that we perform personal hygienic responsibilities—washing dishes or changing automotive oil—in addition to the possible psychological rewards that come from protection—even if one does not act to avoid clear and present dangers.

In sum, our results suggest that, when articulating an IS security threat, individuals do not experience fear appeals in a manner consistent with contemporary fear appeal theory. This neuroscience evidence questions current implementations of fear appeals in IS security. Instead of trying to make the threats seem more threatening, researcher and practitioners should also investigate methods for making recommended responses more appealing. The implications are that perhaps fear appeal theory, though it is an effective lens for explaining responses to articulated threats of cancer, amputation, or death, is not as readily applicable to addressing threats to, for example, one’s identity, hard drive crashes, or malware.

5.1 Limitations and Future Research Opportunities

Given that each research method embodies specific advantages and disadvantages in terms of its rigor and relevance and each data-collection method exhibits conflicts between the simultaneous goals of achieving generalizability, precision, and realism (McGrath, 1995), we could not perfectly match the stimuli encountered in the real world with our lab experiment, and we favored fMRI precision over a study of exact realism in situ. Future research should broaden the group of computer users whose neural activity the research observes. Future research efforts should also attempt to broaden insiders’ exposure to various IS security stimuli, such as other threat-response pairs, including data loss (data backup, password theft) password hygiene, and/or portable data device theft (data encryption). Accordingly, we cannot definitively identify how fear appeals actually operate outside the lab in the real world; we encourage further research in this area with improved experimental paradigms and expanded samples.

Further, future scholars can evaluate other salient factors in cognitively assessing computer security threats and recommended responses. One might study dispositional and cultural factors in the context of neural responses to security-related stimuli. One could contrast the neural activity of experienced computer users with that of novices. Researchers could also explore other related factors in this nomologic net.

6 Conclusion

Organizations must minimize the threats to the security of information systems, which includes those threats caused by unmotivated or careless insiders. Firms target insiders via security awareness, training, and education (SETA) programs, which includes using persuasive communications such as fear appeals, but, for these efforts to succeed, we need a deeper understanding of the impact of threat and response stimuli on human cognitions and affects. Whereas fear appeal theory has historically provided much of this understanding, recent studies suggest that fear appeal theory and reality do not align. Our research is a first effort at investigating this contradiction via functional magnetic resonance imaging (fMRI) data-collection protocols. The data indicate that appraisals of IS security threats have little to do with successfully applying fear appeals. Though the stated threats in a fear appeal stimulate self-referencing cognition, they do not elicit fear. Furthermore, perceptions of self-efficacy are seemingly instrumental in bolstering the impact of fear appeals in this context, which suggests that training about the desirability of certain actions would be more effective in encouraging protective behavior than threats. We need more work, but our findings suggest that this domain is a fruitful area for research that can produce insights into insider security behavior modification that benefit both researchers and practitioners.

Acknowledgements

We thank the organizers and participants of the Interdisciplinary Symposium on Decision Neuroscience and Gmunden Retreat on NeuroIS for their comments and support. We also acknowledge the research support of the Mississippi State College of Business and the Mississippi State Distributed Analytics and Security Institute (DASI).

References

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

Andersson, J. L., Jenkinson, M., & Smith, S. (2007). Non-linear optimization (FMRIB technical report TR07JA1). Oxford, UK: University of Oxford FMRIB Centre.

Aue, T., Hoeppli, M.-E., Piguet, C., Hofstetter, C., Rieger, S. W., & Vuilleumier, P. (2015). Brain systems underlying encounter expectancy bias in spider phobia. *Cognitive, Affective, & Behavioral Neuroscience*, *15*(2), 335-348.

Balsters, J. H., Whelan, C. D., Robertson, I. H., & Ramnani, N. (2013). Cerebellum and cognition: Evidence for the encoding of higher order rules. *Cerebral Cortex*, *23*(6), 1433-1443.

Bechara, A., Tranel, D., Damasio, H., Adolphs, R., Rockland, C., & Damasio, A. R. (1995). Double dissociation of conditioning and declarative knowledge relative to the amygdala and hippocampus in humans. *Science*, *269*(5227), 1115-1118.

Beck, K. H., & Frankel, A. (1981). A conceptualization of threat communications and protective health behavior. *Social Psychology Quarterly*, *44*, 204-217.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1042.

Bhatt, M., & Camerer, C. F. (2005). Self-referential thinking and equilibrium as states of mind in games: fMRI evidence. *Games and Economic Behavior*, *52*(2), 424-459.

Casey, M. K. (1995). *Fatalism and the modification of the extended parallel process model*. Paper presented at the Speech Communication Association, San Antonio, Texas.

Clemente, M., Rey, B., Alcañiz, M., Rodríguez-Pujadas, A., Breton-Lopez, J., Barros-Loscertales, A., Banos, R. M., Botella, C., Alcaniz, M., & Avila, C. (2013). *fMRI assessment of small animals' phobia using virtual reality as stimulus*. Paper presented at the 7th International Conference on Pervasive Computing Technologies for Healthcare.

Compeau, D., Marcolin, B., Kelley, H., & Higgins, C. (2012). Generalizability of information systems research using student subjects—a reflection on our practices and recommendations for future research. *Information Systems Research*, *23*(4), 1093-1109.

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

Crossler, R. E. (2010). *Protection motivation theory: Understanding determinants to backing up personal data.* Paper presented at the 2010 43rd Hawaii International Conference on System Sciences.

Dale, A. M. (1999). Optimal experimental design for event-related fMRI. *Human Brain Mapping*, *8*(2-3), 109-114.

Darwin, C. (1877). A biographical sketch of an infant. *Mind*, 2(7), 285-294.

Dejong, W., & Wallack, L. (1999). A critical perspective on the drug czar's antidrug media campaign. *Journal of Health Communication*, *4*(2), 155-160.

Dilger, S., Straube, T., Mentzel, H.-J., Fitzek, C., Reichenbach, J. R., Hecht, H., Krieschel, S., Gutberlet, I., & Miltner, W. H. (2003). Brain activation to phobia-related pictures in spider phobic humans: An event-related functional magnetic resonance imaging study. *Neuroscience Letters*, *348*(1), 29-32.

Dillard, J. P., Plotnick, C. A., Godbold, L. C., Freimuth, V. S., & Edgar, T. (2006). The multiple affective outcomes of AIDS PSAs: Fear appeals do more than scare people. *Communications Research*, *23*(1), 44-72.

Dimoka, A. (2012). How to conduct a functional magnetic resonance (fMRI) study in social science research. *MIS Quarterly*, *36*(3), 811-840.

Dimoka, A., Banker, R. D., Benbasat, I., Davis, F. D., Dennis, A. R., & Gefen, D. (2012). On the use of neurphysiological tools in IS research: Developing a research agenda for neuroIS. *MIS Quarterly*, *36*(3), 679-702.

Dimoka, A., Pavlou, P. A., & Davis, F. D. (2011). Research commentary—neuroIS: The potential of cognitive neuroscience for information systems research. *Information Systems Research*, 22(4), 687-702.

Dinh-Williams, L., Mendrek, A., Dumais, A., Bourque, J., & Potvin, S. (2014). Executive-affective connectivity in smokers viewing anti-smoking images: An fMRI study. *Psychiatry Research: Neuroimaging*, *224*(3), 262-268.

Ernst & Young. (2014). *Get ahead of cybercrime*. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

Fry, R. B., & Prentice-Dunn, S. (2005). Effects of coping information and value affirmation on responses to a perceived health threat. *Health Communication*, *17*(2), 133-147.

Fullana, M., Harrison, B., Soriano-Mas, C., Vervliet, B., Cardoner, N., Àvila-Parcet, A., & Radua, J. (2015). Neural signatures of human fear conditioning: an updated and extended meta-analysis of fMRI studies. *Molecular Psychiatry*.

Gordon, M. E., Slade, L. A., & Schmitt, N. (1986). The “science of the sophomore” revisited: From conjecture to empiricism. *Academy of Management Review*, *118*(1), 191-207.

Greve, D. N., & Fischl, B. (2009). Accurate and robust brain image alignment using boundary-based registration. *Neuroimage*, *48*(1), 63-72.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203-236.

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

Hilbert, K., Evens, R., Maslowski, N. I., Wittchen, H.-U., & Lueken, U. (2014). Fear processing in dental phobia during crossmodal symptom provocation: An fMRI study. *BioMed Research International*.

Hopfinger, J. B., Buonocore, M. H., & Mangun, G. R. (2000). The neural mechanisms of top-down attentional control. *Nature Neuroscience*, *3*(3), 284-291.

Hovland, C., Janis, I. L., & Kelly, H. (1953). *Communication and persuasion*: New Haven: Yale University Press.

Im, G., & Baskerville, R. (2005). A longitudinal study of information systems threat categories: The enduring problem of human error. *The DATA BASE for Advances in Information Systems*, *36*(4), 68-79.

Janis, I. L. (1967). Effects of fear arousal on attitude change: Recent developments in theory and experimental research. *Advances in Experimental Social Psychology*, *3*, 166-225.

Janis, I. L., & Feshbach, S. (1953). Effects of fear-arousing communications. Jo*urnal of Abnormal and Social Psychology*, *48*(1), 78-92.

Jenkinson, M., Bannister, P., Brady, M., & Smith, S. (2002). Improved optimization for the robust and accurate linear registration and motion correction of brain images. *Neuroimage*, *17*(2), 825-841.

Jenkinson, M., & Smith, S. (2001). A global optimisation method for robust affine registration of brain images. *Medical Image Analysis*, *5*(2), 143-156.

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

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

Klingner, C. M., Hasler, C., Brodoehl, S., Axer, H., & Witte, O. W. (2013). Perceptual plasticity is mediated by connectivity changes of the medial thalamic nucleus. *Human Brain Mapping*, *34*(9), 2343-2352.

LaBar, K. S., Gatenby, J. C., Gore, J. C., LeDoux, J. E., & Phelps, E. A. (1998). Human amygdala activation during conditioned fear acquisition and extinction: a mixed-trial fMRI study. *Neuron*, *20*(5), 937-945.

Larson, C. L., Schaefer, H. S., Siegle, G. J., Jackson, C. A., Anderle, M. J., & Davidson, R. J. (2006). Fear is fast in phobic individuals: amygdala activation in response to fear-relevant stimuli. *Biological Psychiatry*, *60*(4), 410-417.

Lawrence, N. S., Hinton, E. C., Parkinson, J. A., & Lawrence, A. D. (2012). Nucleus accumbens response to food cues predicts subsequent snack consumption in women and increased body mass index in those with reduced self-control. *Neuroimage*, *63(1)*, 415-422.

Lee, J., Crossler, R., & Warkentin, M. (2013). *Implications of monitoring mechanisms on bring your own device (BYOD) adoption*. Paper presented at the 2013 International Conference on Information Systems, Milan, Italy.

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

Leventhal, H. (1970). Findings and theory in the study of fear communications. *Advances in Experimental Social Psychology*, *5*, 119-186.

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

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71-90.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394-413.

Lovecraft, H. P. (1945). *Supernatural horror in literature*. New York: Dover.

McGrath, J. E. (1995). Methodology matters: Doing research in the behavioral and social sciences. In R. Baecker & W. A. S. Buxton (Eds.), *Readings in human-computer interaction: An interdisciplinary approach* (2nd ed., pp. 152-169). San Mateo, CA: Morgan Kaufmann Publishers.

McGuire, W. J. (1968). Personality and susceptibility to social influence. In E. Borgatta & W. Lambert (Eds.), *Handbook of personality theory and research* (pp. 1130-1187). Chicago: Rand McNally.

McGuire, W. J. (1969). The nature of attitudes and attitude change. In G. Lindzey & E. Aronson (Eds.), *The handbook of social psychology* (pp. 136-314). Reading: Addison-Wesley.

Matthews, S. C., Simmons, A. N., Lane, S. D., & Paulus, M. P. (2004). Selective activation of the nucleus accumbens during risk-taking decision making. *Neuroreport*, *15(13)*, 2123-2127.

Mewborn, C. R., & Rogers, R. W. (1979). Effects of threatening and reassuring components of fear appeals on physiological and verbal measures of emotion and attitudes. *Journal of Experimental Social Psychology*, *15*(3), 242-253.

Morris, J. S., Frith, C. D., Perrett, D. I., Rowland, D., Young, A. W., Calder, A. J., & Dolan, R. J. (1996). A differential neural response in the human amygdala to fearful and happy facial expressions. *Nature*, *383*(6603), 812-815.

Northoff, G., Heinzel, A., de Greck, M., Bermpohl, F., Dobrowolny, H., & Panksepp, J. (2006). Self-referential processing in our brain—a meta-analysis of imaging studies on the self. *Neuroimage*, *31*(1), 440-457.

Phelps, E. A., O'Connor, K. J., Gatenby, J. C., Gore, J. C., Grillon, C., & Davis, M. (2001). Activation of the left amygdala to a cognitive representation of fear. *Nature Neuroscience*, *4*(4), 437-441.

Ponemon Institute. (2012a). *2011 cost of data breach study*. Retrieved from http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf

Ponemon Institute. (2012b). *2013 state of the endpoint*. Retrieved from https://www.ponemon.org/local/upload/file/2013%20State%20of%20Endpoint%20Security%20WP_FINAL4.pdf

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

PWC. (2015). *Managing cyber risks in an interconnected world: Key findings from the global state of information security survey 2015*. Retrieved from http://www.pwc.com/gsiss2015

Richardson, R. (2011). *CSI/FBI computer crime and security survey*. San Francisco: Computer Security Institute.

Riedl, R., Banker, R. D., Benbasat, I., Davis, F. D., Dennis, A. R., & Dimoka, A. (2010). On the foundations of neuroIS: Reflections on the Gmunden Retreat 2009. *Communications of the Association for Information Systems*, *27*, 243-264.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *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 protected motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153-176). New York, NY: The Guilford Press.

Roskos-Ewoldsen, D. R., Yu, H. J., & Rhodes, N. (2004). Fear appeal messages affect accessibility of attitudes toward the threat and adaptive behaviors. *Communication Monographs*, *71*(1), 49-69.

Rubin, R. T., Mandell, A. J., & Crandall, P. H. (1966). Corticosteroid responses to limbic stimulation in man: localization of stimulus sites. *Science*, *153*(3737), 767-768.

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.

Scharmüller, W., Übel, S., Leutgeb, V., Schoengassner, F., Wabnegger, A., & Schienle, A. (2014). Do not think about pain: Neural correlates of attention guiding during visual symptom provocation in dental phobia—an fMRI study. *Brain Research*, *1566*, 69-76.

Schienle, A., Scharmüller, W., Leutgeb, V., Schäfer, A., & Stark, R. (2013). Sex differences in the functional and structural neuroanatomy of dental phobia. *Brain Structure and Function*, *218*(3), 779-787.

Smith, S. M. (2002). Fast robust automated brain extraction. *Human Brain Mapping*, *17*(3), 143-155.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133.

Stephenson, M. T. (1993). *A subliminal manipulation of the extended parallel process model* (unpublished master’s thesis). Texas A&M University.

Sutton, S. R. (1982). Fear-arousing communications: A critical examination of theory and research. In J. R. Eiser (Ed.), *Social psychology and behavioral medicine* (pp. 303-337). London: Wiley.

Tung, K.-C., Uh, J., Mao, D., Xu, F., Xiao, G., & Lu, H. (2013). Alterations in resting functional connectivity due to recent motor task. *Neuroimage*, *78*, 316-324.

Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476-486.

Wall, D. S. (2011). *Organizational security and the insider threat: Malicious, negligent and well-meaning insiders* (white paper). Retrieved from https://www4.symantec.com/Vrt/offer?a_id=108920

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 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*, *58*(4), 329-349.

Woolrich, M. W., Jenkinson, M., Brady, J. M., & Smith, S. M. (2004). Fully Bayesian spatio-temporal modeling of fMRI data. *IEEE Transactions on Medical Imaging*, *23*(2), 213-231.

Woon, I., Tan, G.-W., & Low, R. (2005). *A protection motivation theory approach to home wireless security*. In *Proceedings of the International Conference on Information Systems*.

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*(6), 2799-2816.

Zilverstand, A., Sorger, B., Sarkheil, P., & Goebel, R. (2015). fMRI neurofeedback facilitates anxiety regulation in females with spider phobia. *Frontiers in Behavioral Neuroscience*, *9*, 148.

Appendix A: Language Found in Fear Appeal Stimuli

Table A1. Language Found in Fear Appeal Stimuli

Threat	Neutral statements	Threat statements	Response statements
Theft	Your computer case might be made from plastic	Your data are in danger of being stolen	You should always encrypt and lock your computer
Negligence	Your hard drive can store much data	You may accidentally infect your own computer	You should be careful in opening attachments
Website defacement	Your computer can display text and graphics	Your website may be defaced by hackers	You should update your website's security controls
Viruses	Your computer keyboard contains less than 100 keys	Your computer may be infected by a virus	You should run antivirus programs on your computer
Computer theft	You may give away at least one computer	Your computer is in danger of being stolen	You should try to change your password frequently
Computer overheating	Your cost of computer ownership has decreased	Your computer may overheat if not cooled	You should not block your computer's fan
Earthquakes	You may purchase USB drives at many locations	Your computer may be damaged in an earthquake	You should regularly back up your computer's data

Appendix B: Epilogue

The extant IS security research has not investigated security behaviors with fMRI research methods, and research has not examined the true role of fear in fear appeal message processing from a neuroscience perspective. Accordingly, we leveraged contemporary fear appeal theory and recent studies outside of the IS security field to guide our expectations. The suggestion that responses to threats do not elicit a true fear response represents a potential paradigm shift in the study of fear appeal use in IS security research and practice. IS scholars might never have thought of investigating this research direction in the absence of fMRI observations because only one recent study, Johnston et al. (2015), even suggests this direction. Our work represents a significant step in a new direction. But caution is warranted in this endeavor because there are many more activities the brain can perform than regions that we can identify, so it is necessarily the case that some regions are active in response to many different situations.

Appendix C: Detailed List of Activations

Table C1. Contrast Threat > Neutral

Cluster index	Number of voxels	P-value of entire cluster	Maximum Z-Score	Coordinates of voxel of maximum Z-score in MNI152 space
4	4806	9.84E-13	4.11	16, 54, 34
3	1967	1.67E-06	4.58	-2, -82, 14
2	1436	4.59E-05	4.34	-56, -50, 46
1	1289	0.000124	4.16	46, -58, 26

Table C2. Local Maxima (Areas of highest Z-score in each cluster) MNI152 Coordinates

Cluster index	Z	x	y	z	Region
4	4.11	16	54	34	Frontal pole
4	4.08	16	24	58	Superior frontal gyrus
4	4.01	-8	32	38	Paracingulate gyrus
4	3.9	2	30	44	Paracingulate gyrus
4	3.88	-2	32	40	Paracingulate gyrus
4	3.88	18	44	38	Frontal pole
3	4.58	-2	-82	14	Supracalcarine cortex
3	4.03	-14	-82	2	Intracalcarine cortex
3	3.95	-10	-80	16	Intracalcarine cortex
3	3.95	-16	-78	2	Intracalcarine cortex
3	3.95	0	-78	16	Supracalcarine cortex
3	3.83	4	-80	6	Intracalcarine cortex
2	4.34	-56	-50	46	Supramarginal gyrus
2	4.09	-58	-54	38	Angular gyrus
2	4.08	-52	-56	38	Angular gyrus
2	4.02	-58	-48	26	Supramarginal gyrus
2	3.95	-54	-48	30	Supramarginal gyrus
2	3.9	-36	-56	40	Angular gyrus
1	4.16	46	-58	26	Angular gyrus
1	3.8	50	-62	42	Lateral occipital cortex
1	3.76	44	-62	44	Lateral occipital cortex
1	3.74	46	-54	36	Angular gyrus
1	3.65	44	-54	32	Angular gyrus
1	3.6	44	-62	48	Lateral occipital cortex

Table C3. Contrast Response > Neutral

Cluster index	Number of voxels	P-value of entire cluster	Maximum Z-score	Coordinates of voxel of maximum Z-score in mni152 space
6	3709	4.13E-11	4.12	-8, -60, 40
5	1990	5.96E-07	4.87	-48, -62, 40
4	1406	2.90E-05	3.91	16, -84, -22
3	1144	0.000194	4.52	-34, 58, 6
2	924	0.00107	3.97	26, 56, 8
1	818	0.00257	3.45	48, -60, 40

Table C4. Local Maxima (Areas of highest Z-score in each cluster) MNI152 Coordinates

Cluster index	Z-score	X	Y	Z	Region
6	4.12	-8	-60	40	Precuneous cortex
6	3.98	-6	-70	38	Precuneous cortex
6	3.93	2	-66	38	Precuneous cortex
6	3.85	-10	-70	24	Precuneous cortex
6	3.82	2	-72	50	Precuneous cortex
6	3.77	6	-74	42	Precuneous cortex
5	4.87	-48	-62	40	Lateral occipital cortex
5	4.09	-50	-54	48	Angular gyrus
5	4.08	-52	-62	36	Lateral occipital cortex
5	3.87	-54	-62	40	Lateral occipital cortex
5	3.86	-56	-58	36	Angular gyrus
5	3.81	-52	-62	26	Lateral occipital cortex
4	3.91	16	-84	-22	Occipital fusiform gyrus
4	3.87	8	-82	-20	Lingual gyrus
4	3.67	12	-82	-20	Occipital fusiform gyrus
4	3.54	32	-70	-38	White matter
4	3.49	40	-66	-28	White matter
4	3.47	30	-58	-30	White matter
3	4.52	-34	58	6	Frontal pole
3	4.39	-30	54	4	Frontal pole
3	3.91	-34	50	8	Frontal pole
3	3.65	-26	58	6	Frontal pole
3	3.62	-28	50	18	Frontal pole
3	3.59	-24	52	28	Frontal pole

About the Authors

Merrill Warkentin is Professor of MIS and the Drew Allen Endowed Fellow in the College of Business at Mississippi State University. His research, primarily on the impacts of organizational, contextual, and dispositional influences on individual behaviors in the context of information security and privacy, has appeared in MIS Quarterly, Decision Sciences, European Journal of Information Systems, Decision Support Systems, Information Systems Journal, and others, and he is the author or editor of seven books. His 250+ published manuscripts include over 60 peer-reviewed journal articles. He has served as SE and AE for *MIS Quarterly* and AE for *Information Systems Research*, *European Journal of Information Systems*, *Information & Management,* and other journals. He is Senior Editor of the *AIS Transactions on Replication Research* and an Eminent Area Editor for *Decision Sciences*. He has held leadership positions at AIS, DSI, IFIP, and ACM. His work has been funded by NATO, NSF, NSA, DoD, Homeland Security, IBM, and others. He has chaired several international conferences and will be the Program Co-Chair for the 2016 AIS Americas Conference on Information Systems (AMCIS).

Eric Walden is the James C. Wetherbe Professor of Information Systems and Quantitative Sciences, and Director of Data Science Programs at Texas Tech's Rawls College of Business. He is also a self-taught neuroscientist who enjoys studying how the human brain interacts with information technology.

Allen C. Johnston is an Associate Professor and the Director of the MS MIS program in the Collat School of Business at the University of Alabama at Birmingham. His research has been in the area of information assurance and computer security and can be found in such outlets as MIS Quarterly, European Journal of Information Systems, DATA BASE for Advances in Information Systems, and CACM. He currently serves as AE for *European Journal of Information Systems*, *Decision Sciences Journal*, and the *Journal of Information Privacy and Security*, and he serves on the Editorial Review Board for *DATABASE for Advances in Information Systems*. He is a founding member and current Vice Chair of the IFIP Working Group on Information Systems Security Research (WG8.11/11.13) and serves on the administrative board for the UAB Comprehensive Neuroscience Center. He has also served as a visiting professor or invited speaker at several universities and companies in the US and abroad.

Detmar W. Straub is the IBIT Distinguished Visiting Professor at Temple University's Fox School and a distinguished visiting professor at the Korea University Business School. He is also a Regents Professor Emeritus of the University System of Georgia. Formerly holding a professorship in the CIS Department of the Robinson School of Business at Georgia State University, he has conducted research in the areas of information security, e-Commerce, technological innovation, international IT studies, and IS research methods. He holds a DBA in MIS from Indiana and a PhD in English from Penn State. He has more than 200 publications appearing in many top business journals and other venues. He was the Editor-in-Chief of *MIS Quarterly* from 2008-2012. Finally, he was the 2008 winner of the Alumni Distinguished Professor Award at Georgia State University and, in 2012, was awarded a LEO by the Association for Information Systems for lifetime achievement in the field of information systems.