DECISION SCIENCES
A JOURNAL OF THE DECISION SCIENCES INSTITUTE

Decision Sciences
Volume 00 Number 0
xxxx 2018

Speak their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making*

Allen C. Johnston†
University of Alabama, Information Systems, Statistics, and Management Science, Tuscaloosa, AL 35487, e-mail: ajohnston@cba.ua.edu

Merrill Warkentin
Mississippi State University, Mgmt & Info Systems, Mississippi State, MS 39762, e-mail: m.warkentin@msstate.edu

Alan R. Dennis
Indiana University, Operations and Decision Technologies, Bloomington, IN 47405, e-mail: ardennis@indiana.edu

Mikko Siponen
University of Jyväskylä, Information Technology, 40014 Jyväskylä, Finland, e-mail: mikko.t.siponen@jyu.fi

ABSTRACT

Employee disinterest in information security remains one of the greatest impediments to effective information security management programs. How can organizations enhance the persuasiveness of the information security messages used to warn employees of threats and encourage employees to take specific actions to improve their security? We use fear appeal theory and the elaboration likelihood model to argue that security messages presented using more personally relevant language are more likely to induce employees to engage in the recommended protective security behaviors. Our strategy uses organization identification theory to segment employees into two groups and then develops security messages that use language aligned with each of the two segments. We tested this strategy within a large U.S. organization, and found that employees were more likely to consider and act upon messages that used language aligned with their organizational identification than messages using language not aligned. The effect size was large. Our results show that subtly changing less than a dozen words in the way a security message was presented without changing its substantive content (e.g., using "our" instead of "your") has both significant and meaningful effects on how employees think about and respond to it. [Submitted: August 27, 2017. Revised: February 25, 2018. Accepted: June 12, 2018.]

*An earlier version of this manuscript was presented at the 2010 IFIP Dewald Roode Workshop on Information Systems Security Research in Boston, Massachusetts.

†Corresponding author

Subject Areas: Fear Appeal Theory, Information Security, Persuasive Message Strategy, Rhetoric, and Rhetorical Theory.

INTRODUCTION

Ensuring the security of information resources is an important task for individuals and organizations in today's global, data intensive business environments. Information security policies present many technical solutions (e.g., email encryption and anti-virus) and procedural guidelines (e.g., lock computer and choose strong passwords), but it is widely reported that employees do not comply with the policies or deliberately bypass them (e.g., craft easy-to-guess passwords) (D'Arcy, Hovav, & Galletta, 2009; Puhakainen & Siponen, 2010; Willison & Warkentin, 2013; D'Arcy, Herath, & Shoss, 2014). Generally speaking, the problem is not that the employees want to harm the company, but rather that they are not sufficiently motivated to comply with the information security policies presented to them (Puhakainen & Siponen, 2010; Siponen, Mahmood, & Pahnila, 2014; Johnston, Warkentin, & Siponen, 2015). Did you carefully read the last email you received from your IT department about security?

Thus, one key question facing information security practitioners and scholars is how to motivate employees to engage in good information security behaviors (Guo, Yuan, Archer, & Connelly, 2011; Stahl, Doherty, & Shaw, 2012). Many approaches have been suggested (Chen, Ramamurthy, & Wen, 2012), including threat of sanctions (D'Arcy & Herath, 2011; D'Arcy & Devaraj, 2012), user involvement and discursive education (Karjalainen & Siponen, 2011), repeated warnings (Anderson, Vance, Kirwan, Jenkins, & Eargle, 2016), changing organizational culture (Hu, Dinev, Hart, & Cooke, 2012), and justifying information security behavior against common excuses or neutralizations (Siponen & Vance, 2010; Barlow, Warkentin, Ormond, & Dennis, 2013). Yet, despite these attempts, industry studies still routinely conclude that employee behavior is the largest single root cause of security breaches, and most times, it is an unintentional failure to follow good security practices, not deliberate malfeasance (EY, 2017; PricewaterhouseCoopers, 2017).

One common approach for encouraging employees to engage in good information security practices is the use of messages to persuade employees to perform a specific set of behaviors (Johnston & Warkentin, 2010; Puhakainen & Siponen, 2010; Johnston et al., 2015). Many security messages are designed using fear appeal theory (Ruiter, Kessels, Peters, & Kok, 2014). Fear appeals have the goal of "scaring" employees into performing the recommended actions to protect against a specific threat (Johnston & Warkentin, 2010; Puhakainen & Siponen, 2010; Johnston et al., 2015). Recent fear appeal research suggests that the key to successful communication is to ensure that the communicated threat and recommended protective response behaviors are personally relevant to the appeal recipients (Johnston et al., 2015). Unfortunately, many employees do not see information security threats as personally relevant (Warkentin, Johnston, Walden, & Straub, 2016) and thus fail to act on them (EY, 2017; PricewaterhouseCoopers,

2017). Further compounding the challenge is the emerging perspective that fear appeal use by scholars and practitioners has diverged from the underlying theories and models used to explain their impact (Boss, Galletta, Lowry, Moody, & Polak, 2015; Johnston et al., 2015).

How we can design consistent, yet personalized, information security-focused fear appeals and ensure that the appeals are effective in eliciting the desired security behavior remains an unresolved question (Ruiter et al., 2014). In this study, we draw upon fear appeal theory and the elaboration likelihood model (ELM) to develop and test a persuasive rhetorical strategy (PRS) for designing more personally relevant information security messages to increase the likelihood that employees will perceive a significant danger and enact the recommended protective security behaviors. Our strategy leverages these theories, along with the personality characteristic adaptations of different segments of an employee population, to design fear appeals better aligned with their inherent preferences for message rhetoric. We argue that when the rhetoric of a message (i.e., the language used to describe the threat and response) matches an employee's preferences for rhetoric, he or she is more likely to be persuaded by the appeal, and therefore will be more likely to engage in its recommended behaviors—compared with an appeal that does not match an employee's preferences.

We empirically assessed the PRS by conducting a field experiment involving organizational employees and fear appeals commonly used to warn employees of a security threat and motivate them to engage in recommended protective behaviors. We found that fear appeals that matched an employee's preferences for rhetoric resulted in perceptions of a more significant threat and a greater likelihood of engaging in the message's recommended protective security actions. For information security scholars, this research presents a new theoretical approach to increasing information security compliance. More generally, this contribution is an important response to recent studies which contend that the most pressing question facing fear appeal use is how to effectively communicate threats so that people attend to the communication (Peters, Ruiter, & Kok, 2014; Ruiter et al., 2014). Our results also provide an important contribution to information security practice, given the widespread use of fear appeals to motivate security compliance in organizational settings, namely, how to craft information security-focused fear appeals to increase their effectiveness.

THEORETICAL FRAMEWORK

Fear appeals and other forms of persuasive messaging have been shown to be an effective means for influencing individual behavior in general (Ruiter et al., 2014) and for information security protective behaviors in particular (Johnston & Warkentin, 2010; Vance, Siponen, & Pahnila, 2012; Johnston et al., 2015). These messages are often communicated via email and other forms of mass organizational communication because they can cost-effectively reach wide audiences. But with mass communication, these messages can easily end up being generic or undifferentiated and subsequently not considered by some members of the target audience because they do not match these members' expectations for the communication, perspectives on the topic of communication, or preferences for how

the communication should be structured (Te'eni, 2001; Johnston, McBride, Carter, & Warkentin, 2016). Fortunately, scholars continue to advance our understanding of effective fear appeal communication strategies (Ruiter et al., 2014) and have provided a solid foundation upon which to enhance their effectiveness even further.

Fear Appeal Theory

Fear appeal theory is not a singular theory, but rather a set of theories that define a fear appeal, its makeup and underlying assumptions, and its effects on an audience's "interest, recall, persuasiveness, and behavior change" (Williams, 2012, p.16). As suggested by this definition, one large portion of research involving fear appeals is focused on the design of persuasive fear appeals, that is, the rhetorical elements described within the fear appeal that make them influential to their target audience (Ruiter et al., 2014). Within this research stream, several recent studies have provided insight as to what constitutes a persuasive fear appeal (Williams, 2012; Peters et al., 2014; Ruiter et al., 2014; Johnston et al., 2015). Ruiter et al. (2014) reviewed six fear appeal studies within the healthcare literature and determined that the most persuasive elements of a fear appeal are self-efficacy, response efficacy, and threat susceptibility. Interestingly, threat severity was not included as a persuasive element unless accompanied by rhetoric designed to encourage self-affirmation and instructions for implementing a threat avoidance recommended response. Peters and colleagues (2014) provide evidence that suggests efficacy rhetoric is critical to the persuasiveness of a fear appeal and interacts with the threat elements in such a way as to mitigate their potentially negative impact. In fact, they advocate for a nonthreatening form of communication when restricted to mass forms of communication, yet also acknowledge that, in practice, fear-inducing communications remain popular and further research into their effective design is critical to their long-term success. Williams (2012) echoes this call for further research on fear appeal design.

There are two important conditions of fear appeals evident from current fear appeal research. First, fear appeals must have personal relevance to their audience if they are to gain the audience's attention and have a chance of influencing their behavior (Johnston et al., 2015). For instance, Angst and Agarwal (2009) found that when recipients had a stronger concern for information privacy, they were more likely to perceive messages advocating electronic health records as having stronger arguments. Second, the persuasiveness of a fear appeal is dependent upon the audience's personality characteristic adaptations, which represent the values, beliefs, habits, preferences, and self-concepts of an individual derived from basic tendencies and external influences (McCrae & Costa Jr, 1999; McAdams & Pals, 2006; Maier, Wirth, Laumer, & Weitzel, 2017). These important conditions of fear appeal design have been frequently violated by users of fear appeals (i.e., security researchers, professionals, and organizational managers) (Peters et al., 2014; Johnston et al., 2015), yet they serve as important prerequisites for fear appeal persuasiveness.

In summary, prior research suggests that the persuasiveness of a fear appeal message depends on whether the recipient perceives it to be relevant, which is strongly influenced by the personality characteristic adaptations of the recipient.

To some extent, the content of the message is fixed, because the goal is to persuade the recipient to comply with a specific element of the organization's security policy; we cannot change the security policy to fit the personality characteristic adaptations of the recipient. To us, this suggests an interesting theoretical opportunity. Can we increase the persuasiveness of a fear appeal message by better aligning its *rhetorical style*—the words that are used to communicate its message, not the security policy content—with the personality characteristic adaptations of its audience? That is, by systematically changing a few words in the message that are not central to the security policy or security behavior that the message espouses, can we increase compliance? If so, then we have another theoretical lever in our toolkit that can be used to increase information security compliance. We begin by considering what makes a message persuasive (ELM), then describe our strategy for using rhetoric to increase persuasiveness, before turning to our hypotheses.

Elaboration Likelihood Model

A predominant theory for understanding the persuasiveness of a message, including fear appeals, is the ELM. ELM is a dual process theory for understanding how we process messages and form perceptual and behavioral outcomes from those messages (Petty & Cacioppo, 1981). ELM contends that there are two distinct routes by which a message is processed. These routes lead to potentially different perceptual and behavioral outcomes.

The first route, called the central route, involves a cognitively intense, critical consideration of a message's core arguments and the quality of the arguments prior to the formation of perceptions and behaviors; when using the central route, an individual may "elaborate" on the message, drawing in related past information and experiences as he or she thinks deeply about the message. Under the central route, the quality of a message's arguments drives its persuasiveness (Petty & Cacioppo, 1981). In general, strong arguments "contain facts that are justified and compelling" (Angst & Agarwal, 2009; p. 346), but argument quality has been conceptualized using a variety of dimensions, including valence (Levin, Schneider, & Gaeth, 1998), and strength (Priester, Wegener, Petty, & Fabrigar, 1999).

The second route, called the peripheral route, involves less cognitive effort; message recipients avoid deep cognitive processing of the message; instead, behavior is primarily driven by peripheral cues (Petty & Cacioppo, 1981; 1986b), such as message completeness (Dutta-Bergman, 2006), attractiveness/image (Lowry et al., 2012), source expertness and trustworthiness (Lowry et al., 2012), comprehensibility, validity, complexity, degree of repetition, novelty, and even quantitativeness (Yalch & Elmore-Yalch, 1984), to name a few. In short, individuals using peripheral route processing mostly overlook the "rational" arguments a message contains, and instead are influenced more by the peripheral cues, not the central content of the message.

Much research in social psychology, health psychology, management, and information systems has examined what constitutes strong arguments when the recipient of a fear appeal uses the central route. For example, argument quality has been measured in terms of message framing (Angst & Agarwal, 2009) and argument structure (Tam & Ho, 2005). The problem is that strong arguments are

most persuasive when they are cognitively processed via the central route. Most individuals are "satisficers" (Simon, 1979) or "cognitive misers" (Taylor, 1981), who attempt to minimize the effort needed to meet their goals (Maheswaran & Chaiken, 1991; Chen, Duckworth, & Chaiken, 1999). The central route requires considerably more cognitive effort than the peripheral route, so the inherent tendency for most people is to avoid expending cognitive effort and attend mostly to the peripheral cues of an appeal (Petty & Cacioppo, 1981; 1986b; Maheswaran & Chaiken, 1991). Only when there is strong motivation will someone use the central route (Petty & Cacioppo, 1981; 1986b; Maheswaran & Chaiken, 1991).

The implication of this is that while we can design strong, logical arguments for why compliance with security policies is important, they will be ineffective unless the fear appeal recipient is motivated to use the central route. We know what factors influence individuals to perceive security threats and act to mitigate them *when they actually think about information security*—that is, when we have their attention and they engage in central route processing of information security-focused fear appeals. The key problem now is in understanding *how to motivate* individuals who have a low inherent interest in information security to pay attention and actively engage in central route processing of information security-focused fear appeals.

ELM research shows that motivation is a key factor influencing whether an individual engages in central route processing or peripheral routing processing (Chaiken, 1979; Petty & Cacioppo, 1980; 1981; Maheswaran & Chaiken, 1991). The personal relevance of a fear appeal to the recipient is one factor that influences the motivation to pay attention to the appeal and, subsequently, consider it via central route processing (Petty, Cacioppo, & Goldman, 1981). That is, fear appeals viewed as relevant by a recipient are more likely to trigger central route processing and receive the necessary consideration and scrutiny to adequately assess its arguments, while fear appeals viewed as less relevant are more likely to be processed using the peripheral route and thus not be afforded the cognitive effort required to analyze its arguments (Burnkrant & Unnava, 1989). In information systems, for example, Bhattacherjee and Sanford (2006) found that the more relevant a message was to the user's job, the more persuasive it was. Angst and Agarwal (2009) found that when recipients had a stronger concern for information privacy, they were more likely to perceive messages advocating electronic health records as having stronger arguments.

Prior research suggests that customizing a message to the recipient's personality characteristic adaptations can increases its effectiveness (Tam & Ho, 2005; Hirsh, Kang, & Bodenhausen, 2012; Wan & Rucker, 2013). For instance, Tam and Ho (2005) found that deliberately matching message style with a recipient's preferences for structure and dialogue is a key element of a web personalization strategy that can be manipulated to increase consumer engagement. Hirsh et al. (2012) determined that message content tailored to the personality profile of a recipient resulted in increased assessments of message effectiveness, while Yu and Shen (2013) demonstrated that messages framed toward individualistic or collectivistic cultural preferences were also more persuasive in promoting preventive behaviors. Wan and Rucker (2013) determined that one's level of confidence either increases

or decreases message processing based on the degree to which the messages are framed concretely (less abstractly).

These prior studies generally suffer from one or more limitations that prevent richer insights into how customizing messages to recipient preferences can enhance message relevance and thus increase the likelihood that recipients use central route processing. For example, some studies provide evidence that message congruence with recipient preferences for rhetorical style and content structure enhances message effectiveness, but they make the assumption that the message is processed using ELM's central route and fail to control for the influence of peripheral route factors on message elaboration (Hirsh et al., 2012; Wan & Rucker, 2013; Yu & Shen, 2013). Other studies provide evidence of ELM central route processing resulting from message/recipient congruence, but use different message content for different recipient preferences (Tam & Ho, 2005; Angst & Agarwal, 2009; Cesario, Corker, & Jelinek, 2013). Other research provides strategies for message framing, but is limited in that the message arguments are not aligned with the preferences of its audience and provide no evidence of central route processing (Donovan & Jalleh, 1999).

We have presented the two ELM routes as mutually exclusive, as is traditional (e.g., see Petty & Cacioppo, 1981; 1986a). However, it is possible that both routes may be activated concurrently (Maheswaran & Chaiken, 1991). For example, when individuals have barely enough knowledge to use the central route, they may rely on both routes as they shift from one to the other (Chen et al., 1999). Likewise, some peripheral cues may influence central route processing (Chen et al., 1999). The two routes may better be thought of as two endpoints on a continuum (Ho & Bodoff, 2014). Although the two routes are usually treated as separate in theory to better enable sharper distinctions, in real life, as is often the case, the distinctions are not as black and white, but rather behavior can be a blend of both routes.

Information security behavioral compliance communication requires carefully designed content that must be consistently applied across all audience segments and a lasting impact of the core message arguments only found via central route processing (Puhakainen & Siponen, 2010). For fear appeals used toward this purpose, the rhetoric used to express content may change to align with the varying interests of audience segments, but the central tenets of the appeals must remain the same. *How* we design consistent, yet personalized, information security-focused fear appeals and ensure that the appeals are effective in eliciting central route processing remains an unresolved question. Indeed, this is a question with which fear appeal scholars continue to grapple (Ruiter et al., 2014).

A PERSUASIVE RHETORICAL STRATEGY FOR EFFECTIVE FEAR APPEAL DESIGN

So, how can we design an information security-focused fear appeal message to use language that is more personally relevant to employees without altering the core tenets of the appeal? Within a large group of individual message recipients, what is relevant to one individual may be irrelevant to others. In essence, the variability of interests and preferences among a group of employees creates an environment

in which a single fear appeal may be relevant to some and irrelevant others. This disparity creates inconsistent responses to the appeal across its audience so that a significant number of employees fail to actively consider the appeal and comply with the security policies it advocates. We argue that it is possible to segment the employee audience into different groups using personality characteristic adaptations that are commonly held by different types of employees and then design fear appeals to communicate the same threats and recommended responses, but with language specific to the different adaptations held within each employee segments (as we will argue in the discussion, before an employee's personality characteristic adaptations are known, the employee can be sent multiple versions of the message to see which form is most effective). Using language consistent with the argument preferences of a particular personality characteristic adaptation or set of adaptations, it is possible to craft distinct messages for distribution to particular employee audiences over a variety of media, including personalized email messages, electronic learning systems (e-learning systems), Intranet portals, and face-to-face communication.

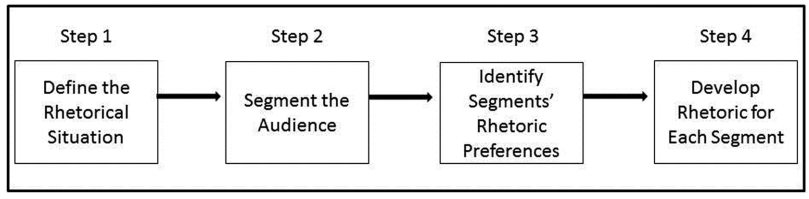
The formal name for language designed to influence is *rhetoric*. A *rhetorical strategy* is a deliberate method of communicating a message using language that is tailored to the message recipient to bring about a desired result (Suddaby & Greenwood, 2005). Rhetorical strategies focus on how messages are created and what words may or may not work in a specific situation (Jones & Livne-Tarandach, 2008) and can be used to influence employees into following the ideals of management (Hartelius & Browning, 2008). There are many rhetorical strategies, including strategies for establishing legitimacy (Suddaby & Greenwood, 2005), civic discovery (Roberts, 1995), and coercion (Andrews, 1973). A PRS is intended to leverage persuasive rhetoric to legitimize or resist a particular set of attitudes or behaviors (Billig, 1996; Suddaby & Greenwood, 2005). A PRS will generally incorporate some combination of appeals to reason (logos), appeals to ethics (ethos), and appeals to emotion (pathos) in the development of persuasive argument rhetoric and will also utilize "institutional vocabularies" that are the structures of words, expressions, and meanings used to express these arguments (Meyer & Rowan, 1977).

Our PRS-informed approach to fear appeal design requires the composition of its arguments using rhetoric tailored to the personality characteristic adaptations of the appeal's audience and their associated preferences for rhetoric. This PRS is focused on how a message is presented to the audience, not on the underlying content of the message. That is, we are composing the language by which security threats and recommended protective behaviors are rhetorically communicated, *not* the content of the message; the description of the threats and recommended actions remain the same, while the language used to communicate them is focused on the audience. As illustrated in Figure 1, our rhetorical strategy for the effective design of fear appeals has four steps: defining the rhetorical situation, segmenting the audience, identifying the segments' rhetoric preferences, and developing rhetoric for each segment. Each step is discussed below.

Step 1: Define the Rhetorical Situation

A rhetorical situation is the setting in which any fear appeal occurs and considers the appeal's source, its target audience, and its content (Bitzer, 1968). In essence,

Figure 1: Rhetorical strategy for effective fear appeal design.



the rhetorical situation establishes the relative boundaries of a communication event and is important to our understanding of the environment in which a fear appeal will be deployed as well as the personal dispositions of the appeal's audience that are most salient within that environment. In our case of designing fear appeals in support of information security communications, the rhetorical situation describes (i) the fact that the appeals will be deployed by management within an organizational setting, (ii) to employees who are involved in securing informational assets, and (iii) will present an information security threat and encourage threat response behaviors as prescribed by the organization's information security policy and procedures. The rhetorical situation provides insight as to the "how" and "why" of the request (Schwartz & Te'eni, 2000), such as asking employees to use strong passwords, encrypt emails, or regularly scan files for viruses.

Step 2: Segment the Audience

Within any organization, there are usually a variety of individuals who have different backgrounds, knowledge, skills, and interests. Audience segmentation is the next step, in which the message author identifies important segments within the target audience that are differentiated in some meaningful way. The goal of this process is to identify characteristics that can be used to customize the rhetoric of the fear appeals to make them more personally relevant to each segment. Strategies for message composition based on audience segmentation are widely used in marketing (Moschis, 2003) and healthcare (Albrecht, 1996). The key difference between this prior work in marketing and the strategy we propose for information security fear appeals is that the content of marketing messages is usually customized for these different segments, such as offering one discount to one customer group and a different discount to another. In the case of information security, it is difficult to change the content; that is, to design one security policy for employees with certain characteristics and different policies for employees with different characteristics. Employees in different job roles can have different security policies, but we are focused on factors such as employee personalities, organizational loyalty, and so on, not job roles. Because security policies generally apply to all employees, the fear appeals must present recommended threat responses that follow best practices and the procedures that embody the organization's security policy. Instead, our strategy focuses on the rhetoric—the words that are used to communicate the single content of the fear appeal.

A classic segmentation strategy is to use demographics, but a more powerful approach is to use personality characteristic adaptations (McCrae & Costa Jr, 1999; McAdams & Pals, 2006; Maier et al., 2017). Personality characteristic adaptations reference one's individualism, propensity for risk, need for cognition, and risk aversion, among many other potential forms and serve as potential leverage points from which to design the rhetoric of a fear appeal's core arguments. The rhetorical situation guides the identification of the audience's personality characteristic adaptations which are most salient. Understanding the salient personality characteristic adaptations enables us to segment the preferences of the audience members to identify the most effective rhetorical language to use in framing the fear appeal. In our case of a rhetorical situation in which information security managers seek to utilize fear appeals to warn of security threats and to recommended protective response behaviors, there are many possible personality characteristic adaptations that could be used to segment the user audience, such as authoritarianism (Lavine, Lodge, & Freitas, 2005), risk aversion (Mahoney, Buboltz, Levin, Doverspike, & Svyantek, 2011), and self-monitoring (Lavine & Snyder, 1996).

Organizational identification is an important personality characteristic adaptation because people with different levels of organizational identification respond differently to different forms of rhetoric (Burke, 1969; Cheney, 1983). Organizational identification is defined as the degree to which an individual identifies with and defines his or her goals and values as similar to those of the organization to which he or she defines himself/herself to be a member (Ashforth & Mael, 1989). Organizational identification is shaped by social identity theory (Tajfel, 1982) which suggests that individuals seek to identify with various referent groups to which they place some value in group membership (Tajfel, 1978; 1981; 1982; Tajfel & Turner, 1985). This identification may manifest itself in behaviors that exhibit organizational loyalty, allegiance, an understanding of obligations to the organization, and selflessness (Ashforth & Mael, 1989). Individuals with a strong sense of organizational identification perceive themselves as one with the organization, and share its common set of values and goals (Ashforth & Mael, 1989).

In the rhetorical situation of information security training, a trainee's sense of organizational identification is salient because it influences the manner in which he or she engages in the learning exercises (Bartlett, 2001) and interprets communication (Meyer, Paunonen, Gellatly, Goffin, & Jackson, 1989). Fear appeals used in support of training activities could be designed to leverage the rhetoric preferences for trainees with both a high and a low sense of organizational commitment. Based on these criteria, we identified two useful audience segments, employees with high organizational identification and those with low organizational identification.

Step 3: Identify Segments' Rhetoric Preferences

The next step is to identify the preferences that different audience segments have for the presentation of security threat and threat response rhetoric. An individual's preference for rhetoric is dependent upon his or her personality characteristic adaptations (Jones & Livne-Tarandach, 2008). The goal here is to utilize what we know from prior research about a particular personality characteristic adaptation to identify a rhetorical framework for argumentation that is appealing to those that

share that adaptation and appropriate for the rhetorical situation. Once a rhetoric preference has been selected, persuasive arguments are designed to appeal to the beliefs or values that individuals with that preference hold (Hartelius & Browning, 2008).

Burke (1969) and Cheney (1983) argued that individuals with high or low organizational identification respond differently based on the degree to which a message uses rhetoric oriented in favor of either the individual or the organization. Employees with a low sense of organizational identification are more responsive to their own needs and interests, whereas employees with a high sense of organizational identification are more responsive to the needs of their organization (employer). Thus, individuals with a high sense of organizational identification are more likely to prefer organizationally oriented rhetoric that uses words such as "us" and "our" and are more likely to be persuaded by it (Burke, 1969; Cheney, 1983). In contrast, individuals with a low sense of organizational identification are more likely to prefer and be persuaded by individually oriented rhetoric that uses words such as "you" and "your" (Burke, 1969; Cheney, 1983). Although this strategy for constructing the rhetoric of a fear appeal to match the recipient's rhetoric preferences is theoretically compelling, we are aware of no research that has examined it.

Step 4: Develop Rhetoric for Each Segment

The next step is to write the appropriate rhetoric for the fear appeals targeted at each segment. Rhetoric is the style by which the content of the appeal is delivered with the goal of persuading the recipient to take the desired actions. In our case, guidance for the rhetoric construction aligned to the individuals with strong organizational identification is provided by Burke (1969) and Cheney (1983) which articulate three tactics for crafting rhetoric to appeal to those with high organization identification. The first invokes the use of the assumed or transcendent "we," whereby the use of terms such as "we" and "our," or instances of the name of the organization, conjures up a sense of sharing or belonging among the message audience. For example, statements such as "We are moving forward in our pursuit of excellence" would serve as an appeal to organization identification. The second tactic calls for an identification through an antithesis approach, whereby the fear appeal urges employees to unite against a common enemy or threat. For example, an organization may release commentary containing passages that highlight threats from "outsiders" such as a "malicious" hacker (Liang, Biros, & Luse, 2016). A third tactic involves invoking a common ground between the individual and the organization by using a language of commonality. For example, communication from an organization's management staff to an employee may state that the organization shares his or her concerns for their safety.

Rhetoric construction tailored to individuals with low organizational identification follows the inverse of the tactics for those with strong organizational identification provided by Burke (1969) and Cheney (1983). For these individuals, the rhetoric should specify the self, using terms such as "you" and "your" and should pit the individual against the threat. For example, the organization should isolate the individual's assets as independent from the organization's

assets and should suggest that this individual must take steps to protect his or her own assets. This tactic also draws on the language of singularity (the opposite of commonality), which appeals to an individual with weak organizational identification.

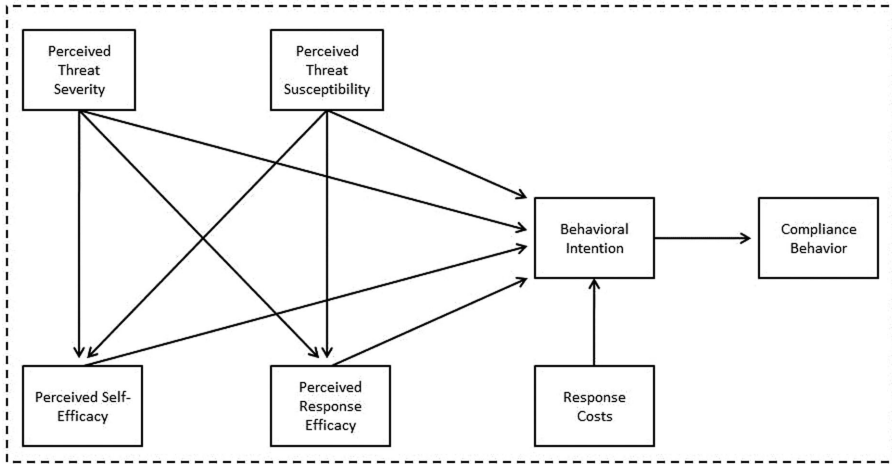
Hypotheses

Our primary research question is whether the use of different styles of rhetoric to communicate a security message is more or less persuasive (without altering the substantive content of the message). Fear appeal theory states that a message is more likely to influence an individual to comply if its substantive content provides five strong convincing arguments: that a threat is severe, that the individual is susceptible to the threat, that the advocated response to mitigate the threat is effective and low cost, and that the individual is capable of implementing the advocated response (i.e., self-efficacy) (Witte, Meyer, & Martell, 2001; Johnston & Warkentin, 2010; Johnston et al., 2015).

Past fear appeal research starts with the assumption that users will think about the fear appeal message, yet, ELM argues that individuals will only think about a message (i.e., use the central route) if they are motivated to invest the cognitive effort needed (Petty et al., 1981). One factor that affects motivation is how personally relevant they perceived the message to be (Petty et al., 1981). If the individual perceives a fear appeal to be personally relevant, he or she will elaborate on the message. That is, he/she will think deeply about the issues communicated in the message and the recommended action presented in the appeal. Conversely, if individuals do not perceive a fear appeal to be personally relevant, they are not motivated to think deeply about its threat or recommended threat response, and therefore will not think deeply about the issues in the message; instead, they will focus more on the peripheral cues of the message, such as font size, message length, and the source of the appeal.

Figure 2 shows the five perceptual factors formed in response to a fear appeal and their influence on behavioral intention and compliance behavior (Johnston et al., 2015). The five perceptual factors in this figure will influence intentions only if the message is processed using the central route, because the arguments contained in a message can only influence intentions and behavior if they are elaborated on using central route (Petty & Cacioppo, 1981; Petty & Cacioppo, 1986a). If the central route is not used, then intentions and behavior are influenced by peripheral cues in the message and the arguments in the message will not be systematically related to intentions and behavior (Petty & Cacioppo, 1981; Petty & Cacioppo, 1986a). That is, if the recipient of a fear appeal elaborates on the rhetoric in the appeal, perceptions of threat, efficacy, and response costs will be formed in accordance with the qualities of the appeal's arguments and will influence behavioral intention and compliance behavior. Conversely, if a recipient of a fear appeal does not elaborate on the rhetoric in the appeal, perceptions of threat, efficacy, response costs, behavioral intention, and compliance will be formed independently of these arguments based on peripheral cues and we will see little relationship between (i) the five perceptual factors and (ii) behavioral intention and compliance. Thus, one indicator of the use of the central versus peripheral route

Figure 2: Perceptual and behavioral responses to information security-focused fear appeals.



is whether the strength of the arguments in the message influences the behavioral intention and compliance: if arguments requiring central route processing influence outcomes, then the central route was used, but if there is little or no relationship between these arguments and the outcomes, then the peripheral route was used (Petty & Cacioppo, 1981; Petty & Cacioppo, 1986a).

In summary, we have three hypotheses. First, we hypothesize that when the rhetoric of a fear appeal aligns with the rhetoric preferences of its audience, the audience members will be more likely to consider the message and therefore the message arguments in the fear appeal about threat severity, threat susceptibility, response efficacy, self-efficacy, and response costs will change the recipient's perceptions. Specifically, the fear appeal arguments will cause the recipient to perceive threat severity, threat susceptibility, response efficacy, and self-efficacy to be higher, and response costs to be lower. In contrast, employees who receive a fear appeal that is not aligned will be less likely to deeply consider it and thus the message will be less persuasive in influencing their perceptions of these five factors. Thus:

H1: *When the fear appeal rhetoric is aligned with the rhetoric preferences of the recipient, the recipient will form higher perceptions of threat severity, threat susceptibility, response efficacy and self-efficacy, and lower perceptions of response costs.*

Second, when the rhetoric of a fear appeal aligns with the rhetoric preferences of its audience, the message elements it contains will be more persuasive; employees' perceptions of the five fear appeal factors will have a strong influence on security compliance. In contrast, when the rhetoric of a fear appeal does not align with the rhetoric preferences of its audience, employees' perceptions of

the five fear appeal factors will little influence on security compliance because peripheral cues will drive compliance. Thus:

> ***H2:*** *When the fear appeal rhetoric is aligned with the rhetoric preferences of the recipient, the recipient's perceptions of threat severity, threat susceptibility, response efficacy, self-efficacy, and response costs will have stronger effects on the recipient's compliance behavior.*

Third, employees who receive fear appeals aligned with their rhetoric preferences are more likely to be persuaded by them. They will be more likely to intend to and actually engage in the compliance behavior advocated by the fear appeal message than employees who receive an appeal whose rhetoric is not aligned. Therefore:

> ***H3:*** *When the fear appeal rhetoric is aligned with the rhetoric preferences of the recipient, the recipient will exhibit greater compliance behavior.*

METHOD

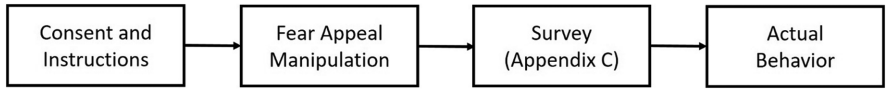
A field experiment was conducted involving employees at a large organization in the southern United States. This organization is relatively large and diverse with over 24,000 employees located in numerous facilities across the country, with the vast majority concentrated in the South. This sampling frame was selected because of the managerial imperative to maximize the effectiveness of security messages to employees due to the critical need for compliance with information security standards and regulatory requirements. U.S. organizations not only face strong ethical and reputational concerns about information privacy and security compliance, they are also subject to stringent regulatory pressures that translate into compliance requirements by each individual employee (Warkentin, Johnston, & Shropshire, 2011).

For this experiment, we used a multigroup experimental design in which we manipulated the pairing of fear appeal rhetoric with participants' organizational identification to form a good alignment versus poor alignment comparison. Good alignment occurred when individuals with high organizational identification received organizationally focused rhetoric and when individuals with low organizational identification received individually focused rhetoric. Poor alignment occurred in the other two conditions: when low organizational identification individuals received organizationally focused rhetoric and when high organizational identification individuals received individually focused rhetoric.

Procedures

Over a three-week period, 725 employees visited the organization's IT helpdesk employee portal without solicitation. The portal described a study designed to help the organization's IT services to better understand their employee base and how they may be better served. Participation was completely voluntary, and no reward was promised for participation. A link was provided that stated that the organization's IT division wanted to "get to know" its clientele better so as to more effectively serve them. If the link was selected, the participant moved forward to

Figure 3: Experimental design flowchart.



the study, beginning with an assessment of the participant's organizational identification. He or she was then randomly assigned to receive either the organizationally focused fear appeal or individually focused fear appeal depending on the balance of each group at that time. After reading the assigned fear appeal, a link was provided that would enable the participant to complete a survey. At the end of the survey was yet another link that, if selected, would lead them to a site where the password could be changed, as recommended in the appeal. Figure 3 depicts the entire flowchart for each participant's experience during the process; please also see the appendices for further details.

Of the 725 employees who visited the IT helpdesk employee portal, 221 employees chose to participate in the study and 204 provided complete and error-free responses. Employees with high organizational identification who received the fear appeal with the organizationally focused rhetoric ($N = 51$) and participants with low organizational identification who received the fear appeal with the individually focused rhetoric ($N = 51$) were categorized into the good alignment group. This group represented the treatment group and had a total of 102 employees. The other employees were classified as poor alignment (high organizational identification with individual rhetoric [$N = 51$], low organizational identification with organizational rhetoric [$N = 51$]). This group represented the control group in the experiment and also had a total of 102 employees.

Participants

Of the 24,000 employees of the organization, 725 were potential subjects of the experiment and 221 actually participated as described below in the procedures section. This represents a 30% response rate. As shown in Table 1, females constituted 56% (115). The majority of participants held a bachelor's degree (127) and almost half (82) had been employed at the organization for at least three years. The 18–29 year age range was most common (100).

Information Security-Focused Fear Appeal Construction

To provide a discrete test of our strategy, we selected the threat of password theft, which continues to warrant attention among scholars (Herath & Rao, 2009; Puhakainen & Siponen, 2010). Passwords are still by far the most common means of user authentication and the number of passwords that users maintain has been increasing (Lee, Chang, Lin, & Wang, 2013). Through obtaining the password, hackers or misusers get access to the systems and all the information under the account. The most common way to obtain passwords is by obtaining access to the password file through malware or using vulnerabilities in operating systems

Table 1: Demographic information.

Demographic	Frequency	Demographic	Frequency
Gender		Experience with computer passwords	
Male	89 (43.63%)	< 6 months	28 (13.73%)
Female	115 (56.37%)	6–12 months	8 (3.92%)
		> 1–2 years	42 (20.59%)
		2–3 years	44 (21.57%)
		> 3 years	82 (40.20%)
Education		Age	
High school	20 (9.80%)	18–29	100 (49.02%)
Some college	15 (7.35%)	30–39	37 (18.14%)
Bachelor's degree	127 (62.25%)	40–49	34 (16.67%)
Master's degree	20 (9.80%)	50–59	26 (12.75%)
Doctorate	22 (21.15%)	60 and over	7 (3.43%)

or applications. Hackers publish these passwords (e.g., Ashley Madison secret dating site's passwords and accounts were hacked and published in the Internet) or sell them on the Internet black market. It reported that users' widely reuse their passwords (using the same password for more than one account) or use modified passwords (using the same password for more than one account with small changes) (Gaw & Felten, 2006; Grawemeyer & Johnson, 2011). The same problem is faced with single sign on systems, not to mention that single sign on passwords is reused in other accounts. Hackers gaining access to such passwords through malware or using vulnerabilities in operating systems or applications get rather universal access to the victims' accounts. Keeping this in mind, use of single sign on systems and/or use of reused password places a high priority on the need to have a random password that is hard to break.

Password theft was also a major concern of managers in this study's participating organization. In constructing our information security-focused fear appeal, we started with the organization's security policy pertaining to password security. The policy included explicit statements about threat severity, threat susceptibility, self-efficacy, response efficacy, and response costs. To highlight the severity of the password theft threat, statements were included in our fear appeal that described the surreptitious capability of individuals and software to capture passwords. We included statements describing the pervasiveness of password theft, thereby highlighting the message recipient's susceptibility to the threat. The recommended action in response to password theft was to change passwords and to use "strong" passwords consisting of at least eight characters that include letters, numbers, and special characters. Consistent with fear appeal theory, we also included statements about the effectiveness and low cost of this response and highlighted the recipient's self-efficacy in executing the response.

We developed two versions of the fear appeal that used different rhetoric (see Appendix A). One version (termed the "organizationally focused fear appeal") was designed following the three tactics for rhetoric described by Burke (1969) and Cheney (1983), including the use of a transcendent "we," identification through

an antithesis, and the use of common ground between the employee and the organization. The fear appeal was designed with argument rhetoric intended to appeal to those with high organizational identification by insinuating a unified fight (employee and organization together) against the common threat, password theft. This message used "we" and the name of the organization repeatedly, and it identified a common enemy ("hackers") and attempted to build common ground. We expected that this fear appeal would have the best alignment for those with high organizational identification.

The other version (termed the "individually focused fear appeal") was designed with rhetoric intended to appeal to those with low organizational identification by implying an individualized struggle for the individual user against an isolated threat. It was identical to the first fear appeal in all ways except it used the language designed to appeal to the individualist by following using personally identifying words such as "you" and "your" and by avoiding the name of the organization. The appeal's rhetoric was designed to isolate the individual and focus the articulated threat against the individual's information assets. This fear appeal would have the best alignment for those with low organizational identification.

Each fear appeal was reviewed by a panel of experts in marketing, communication, and experimental design and was validated as to its proper inclusion of and orientation of rhetoric in support of these strategies. The panel was also asked to evaluate the potential relevance of the appeals to those identifying with the organization and to those with individual interests. Following the panel's review, the appeals were edited according to their suggestions and reviewed repeatedly until all experts were satisfied. A second panel of subject matter experts, comprised of IT professionals, validated the content validity (realism), technical correctness, and consistency with the rhetorical situation. We also included a manipulation check during the execution of the experiment itself to ensure that the organizationally focused fear appeal was perceived by participants to be more oriented to the organization than the individually focused fear appeal. Appendix B describes this manipulation check.

Measures

There were eight measured constructs. The first was the actual behavior of each participant in complying or not complying with the fear appeal that recommended changing passwords. A link was provided that enabled the participant to change his or her password. Actual password change behavior was recorded by monitoring the password change activities of the participant[i]. Password change behavior was assessed by matching the participants' IP addresses and questionnaire timestamps with entries in the password logs maintained by the organization's password management systems. A password change, originating from the IP address of a participant within 5 minutes of the time at which the participant submitted the questionnaire, was considered to be a password behavior change. The 5-minute

[i] The study participants were able to maintain anonymity throughout the experimental process as the entire procedure was conducted through an online survey tool connected to the organization's website. It should be noted that the participants were likely not seeking to change their passwords before the fear appeal manipulation because the password change link is not typically available on the IT help website. Therefore, it is reasonable to presume that the employees visited the website for other reasons.

threshold was based on the professional experience of the system administrator and his awareness of historical patterns of password change behavior on the system. By monitoring this activity, we are capturing actual security compliance behavior, which is missing from the vast majority of information security studies.

Seven latent variables were measured on a questionnaire using multi-item scales drawn from previously validated instruments adapted specifically to the context of this study. All of the measures were assessed using a five-point Likert-type scale, fully anchored by 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree. Organizational identification was measured using Mael and Ashforth's (1992) six-item scale for organizational identification. Participants with a mean above 3.0 across all items of this scale were categorized as having high organizational identification, while those below this value were categorized as having low organization identification. Threat severity, threat susceptibility, self-efficacy, response efficacy, and behavioral intention were each measured using three item reflective scales first established by Witte, Cameron, McKeon, and Berkowitz (1996). Response cost was measured using a six-item measure adapted from the response cost scales provided in both Fruin, Pratt, and Owen (1991) and Tanner et al.'s (1991) studies involving protection motivation outcomes. Prior to the data collection process, content validity for the seven scales was established through the process described by Lawshe (1975), Peter (1981), and MacKenzie, Podsakoff, and Podsakoff (2011), involving an expert panel consisting of five security and quantitative research design experts. Following the expert panel's review, the instrument was modified accordingly.

DATA ANALYSIS AND RESULTS

The following sections detail the data analysis procedures involved in testing the research model, including measurement and structural model analyses and an additional post-hoc analysis. We used AMOS 21.0.0 (Build 1178) to conduct a confirmatory factor analysis (CFA) of the measurement model, followed by tests of the structural model and the associated hypotheses.

Measurement Model Analysis

According to Hair, Anderson, Tatham, and Black (1998), the adequate fit of a model to a data set is established if most model-fit indices match or exceed an accepted standard for model fitness. As indicated in Table 2, all but one of the fit indices for our measurement model matches or exceeds a published standard, thereby suggesting the measurement model has an acceptable level of fit to the data.

Tests of convergent validity, discriminant validity, and reliability were performed for all of the variables involved in the research model, including threat severity, threat susceptibility, self-efficacy, response efficacy, response costs, and behavioral intention. Following a CFA with Varimax rotation, factor loadings were examined to ensure that items loaded cleanly on their intended constructs, and did not cross-load on constructs to which they should not load (Gefen & Straub, 2005). Convergent validity can be established if (i) item loadings on their intended

Table 2: Fit indices for the measurement model.

Fit Indices	Recommended Value	Suggested by Authors	Our Measurement Model
χ^2/df	≤3	Hayduck (1987)	1.98
Goodness of fit index (GFI)	≥0.9	Scott (1991)	0.88
Adjusted for degrees of freedom (AGFI)	≥0.8	Scott (1991)	0.83
Normed fit index (NFI)	≥0.9	Bentler and Bonett (1980)	0.92
Comparative fit index (CFI)	≥0.9	Bagozzi and Yi (1988)	0.96
Root mean square error of approximation (RMSEA)	≤0.08	Bagozzi and Yi (1988)	0.07

Table 3: Convergent validity test results.

Construct	Items	Factor Loadings	Composite Reliability (CR)	Average Variance Extracted (AVE)
Threat severity	TSEV1	0.90	0.873	0.699
	TSEV2	0.92		
	TSEV3	0.83		
Threat susceptibility	TSUS1	0.85	0.793	0.562
	TSUS2	0.78		
	TSUS3	0.82		
Self-efficacy	SEFF1	0.82	0.859	0.677
	SEFF2	0.60		
	SEFF3	0.88		
Response efficacy	RESP1	0.70	0.831	0.628
	RESP2	0.87		
	RESP3	0.89		
Response costs	COST1	0.66	0.900	0.602
	COST2	0.63		
	COST3	0.79		
	COST4	0.82		
	COST5	0.84		
	COST6	0.72		
Behavioral intention	BINT1	0.96	0.989	0.967
	BINT2	0.96		
	BINT3	0.95		

constructs are in excess of 0.50 (Hair et al., 1998); (ii) composite reliability (CR) is above 0.7; and (iii) average variance extracted (AVE) is above 0.50 for each construct (Gefen & Straub, 2005). As shown in Table 3, these conditions have been met. Also, CR scores equal to or greater than 0.70 are considered acceptable indicators of reliability for the measures (Fornell & Larcker, 1981; Gefen & Straub,

Table 4: Reliability and interconstruct correlations.

	Interconstruct Correlations					
Construct	TSEV	TSUS	SEFF	RESP	COST	BINT
TSEV	0.836					
TSUS	0.083	0.750				
SEFF	0.067	–0.056	0.823			
RESP	0.205	–0.026	0.306	0.792		
COST	–0.020	0.169	–0.667	–0.369	0.776	
BINT	0.102	0.294	0.193	0.226	–0.259	0.983

Shaded items are square root of average variance extracted (AVE); off-diagonal elements are correlations between constructs.

Table 5: Cross loadings of measurement items to latent constructs.

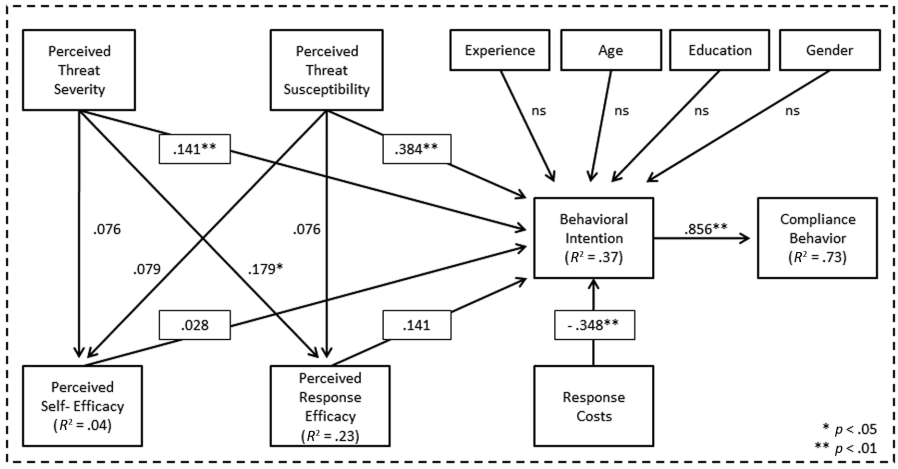
	Component					
Items	TSEV	TSUS	SEFF	RESP	COST	BINT
TSEV1	.895	.093	.061	–.009	.091	–.065
TSEV2	.921	.038	–.006	–.003	.101	.018
TSEV3	.832	–.027	.019	.027	–.007	.179
TSUS1	.026	.850	–.105	–.006	–.017	.166
TSUS2	.042	.781	.056	–.003	.018	.145
TSUS3	.119	.820	.019	.141	–.061	.055
SEFF1	–.235	.026	.818	.018	.262	.074
SEFF2	–.333	.271	.598	.087	.076	–.047
SEFF3	–.310	.038	.883	.033	.130	–.015
RESP1	–.129	.085	.289	.698	–.016	–.045
RESP2	–.157	.061	.055	.865	.118	–.053
RESP3	–.152	.102	.042	.888	.092	.038
COST1	.060	–.126	–.490	.025	.659	.077
COST2	.059	–.049	–.458	.030	.631	.207
COST3	–.298	–.154	–.060	.068	.794	.154
COST4	–.179	–.048	–.204	–.070	.824	.186
COST5	–.161	–.100	–.110	–.041	.845	–.089
COST6	–.124	–.057	–.400	.058	.722	–.127
BINT1	–.126	.148	.092	.023	.087	.960
BINT2	–.123	.131	.073	.056	.094	.965
BINT3	–.101	.153	.096	.034	.088	.953

Extraction method: principal component analysis; rotation method: Varimax with Kaiser normalization.

2005). These values are also provided in Table 4 and suggest an acceptable level of reflective variable reliability.

Discriminant validity for the reflective variables is demonstrated if (i) the square root of each construct's AVE is greater than the interconstruct correlations and (ii) item loadings on their respective constructs are greater than their loadings on other constructs (Fornell & Larcker, 1981). Provided in Tables 4 and 5, respectively, these conditions have been met as well.

Figure 4: Structural model for the good alignment group.

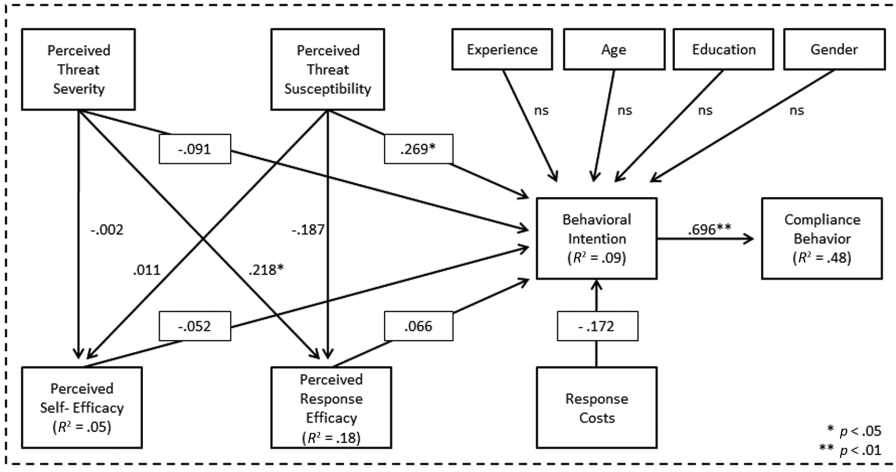


Following the lead of other studies involving multigroup analyses (Hsieh, Rai, & Keil, 2008), we conducted a multigroup measurement invariance analysis to ensure that the measures utilized in this study were being measured consistently across the poor alignment and good alignment groups, thereby permitting path coefficient comparisons. To do so, we again utilized AMOS 21.0.0 (Build 1178) to perform configural and metric invariance analysis (Doll, Raghunathan, Lim, & Gupta, 1995; Steenkamp & Baumgartner, 1998). Configural analysis allows us to test whether measurement item loadings are congeneric across both groups; while, metric invariance analysis provides a test of whether the items have equal loadings between the two groups. Results of the configural invariance analysis reveal that the pattern of item loadings across both the poor alignment and good alignment groups to be congeneric. These results include model fit statistics of CMIN/DF = 1.856, CFI = .916, and RMSEA = 0.065 for the measurement model run with both groups estimated freely. Metric invariance was also established by examining the Chi-squared differences in a constrained and freely estimated model. Results indicate no significance between the two models (p-value > .05), thereby providing additional support for post-hoc path coefficient comparison tests across the two groups.

Structural Model Analysis

Figure 4 shows the structural model for the good alignment group tested using AMOS 21.0.0 (Build 1178). The model-fit indices indicate good fit (CMIN/DF = 1.558, CFI = .954, and RMSEA = 0.074). The results show that all five perceptions significantly influenced behavioral intention ($R^2 = 37\%$), which significantly influenced compliance behavior (R^2 of 73%). None of the control variables of experience, age, education, or gender were significant. We conclude that this pattern

Figure 5: Structural model for the poor alignment group.



of results indicates that, as prior theory argues, participants in the good alignment group processed the information about the five factors in the fear appeal which influenced their intentions and actual behavior.

Figure 5 shows the structural model for the poor alignment group. The model-fit indices indicated a reasonable fit (CMIN/DF = 1.831, CFI = .905, and RMSEA = .08). The results show that only threat susceptibility significantly influenced behavioral intention, but with a low explained variance (R^2 = 9%). The link from intentions to compliance behavior is statistically significant, suggesting that intentions influence behavior (R^2 = 48%), but factors other than perceived threat severity, efficacy, and response costs influence intentions. Similar to the good alignment group model, none of the control variables were significant. It is harder to draw conclusions for the poor alignment group because the results show that their perceptions of the five factors did not materially influence intentions. We conclude that this indicates that participants in this group did not process information about the five factors sufficiently to form consistent perceptions and thus the factors had no meaningful effects on intentions or actual behavior. In short, participants did not consider the fear appeal information to the same extent as the good alignment group because it was not personally relevant.

MultiGroup Analyses of Differences between Poor and Good Alignment Groups

We also compared means between the good alignment group and the poor alignment group. The results, shown in Table 6, indicate that participants formed significantly higher/lower perceptions of the five factors. We therefore conclude H1 is supported. Likewise, participants in the good alignment group were significantly

Table 6: Multigroup analysis results.

Variable	Poor Alignment Group ($N = 102$) Mean	Good Alignment Group ($N = 102$) Std Dev	Significance Mean	Std dev	t-value	p-value
Threat severity	3.000	.4684	3.849	.4970	5.404	.000
Threat susceptibility	2.804	.5753	3.224	.6576	3.203	.001
Self-efficacy	2.833	.6581	3.272	.7457	3.082	.001
Response efficacy	3.004	.6196	3.472	.7479	3.190	.001
Response costs	2.933	.9162	2.679	.8679	2.030	.022
Behavioral intent	2.588	1.056	3.101	1.200	3.241	.001
Compliance behavior[a]	0.20	0.399	0.51	0.502	24.392	.000

[a]The mean value of the binary compliance behavior variable is the percentage of participants performing compliance behavior.

more likely to engage in the recommended compliance behavior than those in the poor alignment group, thus we conclude that H3 is also supported.

We examined the effect sizes for behavioral intentions and compliance behavior between the two groups (poor alignment and good alignment). For behavioral intentions, the coefficient of determination between the two groups was $\Delta R^2 = .28$ which Cohen (1988) calls a large-sized effect ($f^2 = .389$). For compliance behavior, the effect size was $\Delta R^2 = .249$ which is a medium-sized effect ($f^2 = .331$). Thus, we conclude that the differences were meaningful as well as significant. We also assessed whether the path coefficients in the two structural models were significantly different (using AMOS to conduct two-tailed pairwise path coefficient difference tests). All but one of the path coefficients was significantly different between the two groups ($p < .05$); see Table 7. This provides further support that the fit between the message rhetoric and the audience member influences how the message is processed, the extent to which fear appeal message elements influences intentions to comply, and ultimately, how persuasive a message is. We conclude that H2 is supported.

DISCUSSION

Employee disinterest in information security threats and in performing the steps necessary to mitigate the threats poses a great danger to the security of an organization. We developed and tested a theory-based strategy for creating information security fear appeal messages whose rhetoric is more likely to induce them to take action to comply with security policies. An empirical test of the strategy shows that fear appeals are more effective when the rhetoric in the appeals is aligned with the personality characteristic adaptations held by the message recipients than when the rhetoric is not aligned. When there was a good alignment between the fear appeal's rhetoric and the participant's organizational identification, participants were more likely to form significantly higher perceptions of threat severity and susceptibility, significantly higher perceptions of self-efficacy to implement the recommended behavioral response and the efficacy of the response to mitigate the threat, and significantly lower perceptions of the cost of the behavior. Consequently, participants presented with these well-aligned fear appeals were more likely to formulate behavioral intentions to engage in the recommended behaviors presented in the fear appeal. And most importantly, they were more likely to act on those intentions and actually perform the recommended behaviors that the fear appeal advocated.

When there was a poor alignment between the fear appeal's rhetoric and the participant's organizational identification, the appeal was unable to strike a nerve with its intended audience and perceptions of threat severity, self-efficacy, response efficacy, and lower response cost did not influence the audience's behavioral intentions to comply with the policy. Participants failed to see the personal relevance of the message and as a result were not motivated to cognitively process the information about the five factors. As a result, behavioral intentions were driven by factors not accounted for or manipulated in the study. And most importantly, participants were less likely to actually perform the recommended threat response behavior that the fear appeal advocated.

Table 7: Comparison of model paths between groups.

	Poor Alignment Group ($N = 102$)		Good Alignment Group ($N = 102$)		Statistical Comparison of Paths	
Construct	Standardized path coefficient	p-value	Standardized path coefficient	p-value	z-value	p-value
Threat severity → BI	–0.091	$p > .05$	0.141	$p < .01$	2.542	$p < .05$
Threat susceptibility → BI	0.269	$p < .05$	0.385	$p < .01$	2.226	$p < .05$
Self-efficacy → BI	–0.052	$p > .05$	0.028	$p > .05$	0.423	$p > .05$
Response efficacy → BI	0.066	$p > .05$	0.141	$p > .05$	2.431	$p < .05$
Response costs → BI	–0.172	$p > .05$	–0.348	$p < .01$	3.169	$p < .05$

It is important to note that there were no substantive differences in content between the two types of message. There were no differences in the nature of the threat or the nature of the advocated response, and no differences in the myriad of other factors argued to influence compliance, such as sanctions (D'Arcy & Herath, 2011; D'Arcy & Devaraj, 2012), user education (Karjalainen & Siponen, 2011), repetition (Anderson et al., 2016), justification against neutralizations (Siponen & Vance, 2010; Barlow et al., 2013), and so on. The sole difference between the messages was the rhetoric used to communicate the message, whether the message used individually oriented words such as "you" and "yours" or organizationally oriented words such as "us" and "ours."

We believe that this research has the potential to refocus future security research on what to date has received little research attention in explaining employee disinterest in information security threats and the protective behaviors recommended by security managers. Past research has focused on the factors influencing protective security behaviors when employees actively consider security messages (Herath & Rao, 2009; Johnston & Warkentin, 2010; Vance et al., 2012), which is important and necessary research. However, such research is only useful in explaining behavior when employees actually think about the factors shown to influence behavior. We argue that much of the problem with employee disinterest in security concerns seen by security managers today is due to the fact that employees are not motivated to process security messages; because the messages are not personally relevant to them, the key arguments they contain fall on deaf ears and fail to influence behavior. As a result, employee security interests and actions are mostly driven by cues outside of the communication and thus appear somewhat random. We believe that it is time to focus our research on how to enhance the personal relevance of information security-related fear appeals. The current research provides researchers another means by which to design fear appeals to have an impact within this context.

Also, the measurement of actual security behavior is often absent from research due to measurement challenges, leading to well-founded questions concerning the link between intentions and future behaviors. Scholars have questioned not only the link between behavioral intention and actual behavior, but also the validity of measuring self-reported intentions (Straub, 2009). In this study, we measured self-reported intentions on the questionnaire, and then examined actual behavior on the organization's own website in the moments that followed. By not relying on a single source for both the predictor and criterion data, we have minimized the threat of common method variance (Podsakoff & Organ, 1986) and have provided an added degree of rigor. Furthermore, we have pursued the strategy suggested by Straub (2009) and Warkentin et al. (2016) to measure more meaningful actual behaviors of interest rather than intentions.

Limitations

Our study suffers from the usual limitations of field experiments. We studied employees working in one organization. Though we believe this organization and its employees comprised an appropriate and diverse environment for testing our theory, it is possible that they differed in some unknown way from other

organizations. Also, we studied only one personality characteristic adaptation (organizational identification). Although organizational identification is just one of many different personality characteristic adaptations, it is possible that organizational identification is somehow unique and behaves in a manner unlike all the others. Future research should explore other adaptations that could be used to differentiate employee rhetoric preferences, including authoritarianism, individualism, and risk aversion.

It should also be noted that the employees who volunteered to opt-in to the study may have been those who were characterized by greater or lesser organizational identification, thus being unrepresentative of the population of employees at the focal organization. However, participation was controlled for in a way that provided equal representation in the study from those that self-identified as having either high or low degrees of organizational identification. Further, participants were randomly assigned to the treatment and control groups, thereby mitigating this potential for bias. We did not directly ask participants how motivating the fear appeal message was, so we are inferring their level of motivation from their response to other constructs. We compared messages that were well aligned to those that were poorly aligned with the participant's rhetorical style. We did not compare these messages to a "neutral" message that was neither aligned nor misaligned, so it is difficult to assess the extent to which good alignment increases compliance compared to neutral messages. Future research is needed to address this question.

Finally, as with all field experiments, we examined actual behavior in a real organizational setting (not artificial behavior in a laboratory setting) which could have been influenced by a myriad of other factors in the environment, although we used random assignment to mitigate this threat. A longitudinal approach in which the influence of fear appeals over time could be collected should be an important goal of future research. Similar to the habituations to security warnings found by Anderson et al. (2016), responses to fear appeals could exhibit habituation in the long run.

Implications for Research

Despite these limitations, we believe that this research has several implications for future research. First, we believe that our results help to answer the call for more research on how to motivate employees to attend to fear appeals (Peters et al., 2014; Ruiter et al., 2014). Past research has shown fear appeals to have mixed success in inducing people to comply with recommended behavior, whether in general (Peters et al., 2014; Ruiter et al., 2014) or security specific (Johnston et al., 2015). Although the conventional wisdom is that emphasis should be placed on the efficacy components of fear appeals (Peters et al., 2014; Ruiter et al., 2014; Johnston et al., 2015), we believe much of the inconsistency in past research stems from the fact that fear appeals only affect behavior as theorized if recipients are sufficiently motivated to read them and cognitively process the information they contain. If the fear appeal is not seen as personally relevant, then the recipients may disregard it and it will have little impact on behavior. Thus, before we can begin to understand what components of a fear appeal have the greatest impact on behavior, we need to first understand how to motivate the processing of those

components. Our contention and findings partially support Peters et al.'s (2014) arguments that the developers of fear appeals are only partially informed of "the working mechanisms of threatening communication." (pg. 4).

Second, our results show that the same fear appeal content delivered in different rhetorical argument styles has very different effects on cognition and ultimately security behavior depending upon the personality characteristic adaptations of the message recipient. Research involving fear appeals has experienced impressive growth in recent years, both in terms of volume and impact (Ruiter et al., 2014). For the vast majority of these studies, applications of fear appeals assume a "one size fits all" mentality and do not account for audience preferences for rhetoric. This study establishes a need to account for the rhetorical situation of the communication environment and the salient personality characteristic adaptations of the audience members prior to formulating the fear appeal.

Third, an important avenue for future research centers on the notion that we possess numerous personality characteristic adaptations that influence our motivation to use central route processing on the messages we receive. The interactions among personality characteristic adaptations undoubtedly from a complex equation that is not easily solvable, but in understanding it, would allow for even more targeted messaging in support of a desired behavioral outcomes. We found that organizational identification was important in motivating the processing of an organization's information security messages. Future research should examine other personality characteristic adaptations, helping us to understand the dominant adaptations that are most salient within a particular context. Organizational identification may be a very salient personality characteristic adaptation for organizational messages, but only future research can tell.

Finally, another clear limitation of any persuasive message campaign is that the increased effectiveness of information security fear appeals may decay and diminish over time through a process where the message recipients (employees) are not influenced by fear appeals crafted by rhetorical strategies as time passes. Just as SETA programs, in general, exhibit temporal decay, improved fear appeals may similarly lose their increased impact over time. This dynamic process deserves further research to determine and evaluate the impact of time on message effectiveness.

Implications for Practice

We believe this study has important and useful implications for practice. First, our results suggest an overall approach to communicating information security threats and recommended response behaviors to employees. This approach should recognize that different employees have different personality characteristic adaptations which are salient to the context that can provide a leverage point from which to increase the persuasiveness of communication.

Our strategy begins by identifying important segments within the employee audience based on personality characteristic adaptations and then crafting messages that use different rhetoric to communicate the security threat and recommended threat response. More likely, personality characteristic adaptations are not known, so the solution is simple: all employees receive multiple forms of the message.

Eventually, all employees will receive a form of the message that is best suited to their personality characteristic adaptations, which will increase the likelihood of engaging in recommended protective security behaviors.

For example, we have shown that organizational identification is an important personality characteristic adaptation that significantly influences whether employees devote careful attention to a message. Therefore, the simplest place to start is by using organization identification. Security managers should draft a security message as they would normally, then they should revise this base message into two forms. The first version should be written as organizationally focused fear appeal using "we" and placing the organization and the employee working together in a unified fight at the center of the message. Appendix A provides an example. The second version should be written as individually focused fear appeal using "you" and featuring the employee in an individualized struggle against an isolated threat. Appendix A provides an example. Both messages should be sent to all employees several weeks apart. The cost of writing two versions of the message is minimal, as is the cost of sending one additional SETA message.

It is common for organizations to track the response to emails sent to employees (or customers). Thus, over time, the organization can identify which rhetorical style is more effective with each individual employee. Once a database of responses is built, organizations can identify which rhetorical style is most effective for each individual employee. They can then choose to send messages in that one rhetorical style to each employee. As we note above, there are other personality characteristic adaptations beyond organizational identification that could be used to segment employees. Personality characteristic adaptations such as individualism, risk aversion, or authoritarianism might or might not be more effective, depending upon the nature of the SETA message and security behaviors the organization wants to target.

CONCLUSION

Drawing on fear appeal theory and rhetorical theory, this study developed and tested a PRS for crafting information security-focused fear appeals to increase their effectiveness in drawing the interest of employees to threats to their organization and to the recommended actions they can take to protect against the threats. By manipulating the rhetoric of fear appeals to better align with the personality characteristic adaptations held by different segments of employees, it was demonstrated that employee perceptions of threats and the recommended protective actions could be improved. This study provides an important contribution to our understanding of fear appeal use within an organizational context and to our ability to manipulate security communications to enhance their effectiveness. Given that employee disinterest in information security threats and the protective behaviors recommended by security managers continue to plague organizations, the PRS for creating fear appeals developed in this study should inform information security management efforts that include communication with employees. Fear appeals are more effective in attaining the interest of employees and motivating employee behavior if they are developed with an understanding of employee mindsets, personality

characteristic adaptations, and argument preferences. In other words, we must "speak their language."

REFERENCES

Albrecht, T. L. (1996). Advances in segmentation modeling for health communication and social marketing campaigns. *Journal of Health Communication*, *1*(1), 65–80.

Anderson, B. B., Vance, A., Kirwan, C. B., Jenkins, J. L., & Eargle, D. (2016). From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems*, *33*(3), 713–743.

Andrews, J. R. (1973). Coercive rhetorical strategy in political conflict: A case study of the Trent affair. *Communication Studies*, *24*(4), 253–261.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, *33*(2), 339–370.

Ashforth, B. E., & Mael, F. (1989). Social identity theory and the organization. *Academy of Management Review*, *14*(1), 20–39.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, *39*, 145–159.

Bartlett, K. R. (2001). The relationship between training and organizational commitment: A study in the health care field. *Human Resource Development Quarterly*, *12*(4), 335–352.

Bentler, P. M., & Bonett, D. G. (1980). Significant tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin*, *88*(3), 588–606.

Bhattacherjee, A., & Sanford, C. (2006). Influence processes for information technology acceptance: An elaboration likelihood model. *MIS Quarterly*, *30*(4), 805–825.

Billig, M. (1996). *Arguing and thinking: A rhetorical approach to social psychology*. Cambridge, UK: Cambridge University Press.

Bitzer, L. F. (1968). The rhetorical situation. *Philosophy and Rhetoric*, *1*(1), 1–14.

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

Burke, K. (1969). *A rhetoric of motives*. Berkeley, CA: University of California Press.

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

Cesario, J., Corker, K. S., & Jelinek, S. (2013). A self-regulatory framework for message framing. *Journal of Experimental Social Psychology*, *49*(2), 238–249.

Chaiken, S. (1979). Communicator physical attractiveness and persuasion. *Journal of Personality and Social Psychology*, *37*(8), 1387.

Chen, S., Duckworth, K., & Chaiken, S. (1999). Motivated heuristic and systematic processing. *Psychological Inquiry*, *10*(1), 44–49.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157–188.

Cheney, G. (1983). The rhetoric of identification and the study of organizational communication. *Quarterly Journal of Speech*, *69*(2), 143–158.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd edn). Hillsdale: Erlbaum Associates.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, *43*(6), 1091–1124.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658.

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.

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

Doll, W. J., Raghunathan, T. S., Lim, J. S., & Gupta, Y. P. (1995). A confirmatory factor analysis of the user information satisfaction instrument. *Information Systems Research*, *6*(2), 177–188.

Donovan, R. J., & Jalleh, G. (1999). Positively versus negatively framed product attributes: The influence of involvement. *Psychology and Marketing*, *16*(7), 613–630.

Dutta-Bergman, M. J. (2006). Media use theory and internet use for health care. In M. Murero, & R. E. Rice. (Eds.) *The internet and health care: Theory, research, and practice*, New York: Routledge, 83–103.

EY. (2017). Path to cyber resilience: Sense, resist, react. *EY's 19th Global Information Security Survey 2016–2017*.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equations with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50.

Fruin, D. J., Pratt, C., & Owen, N. (1991). Protection motivation theory and adolescents' perceptions of exercise. *Journal of Applied Social Psychology*, *22*(1), 55–69.

Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. *Proceedings of the Second Symposium on Usable Privacy and Security*. Pittsburgh, PA: ACM, 44–55.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*(5), 91–109.

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), 256–267.

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.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate analysis*. Englewood, CA: Prentice Hall International.

Hartelius, E. J., & Browning, L. D. (2008). The application of rhetorical theory in managerial research: A literature review. *Management Communication Quarterly*, *22*(1), 13–39.

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

Hirsh, J. B., Kang, S. K., & Bodenhausen, G. V. (2012). Personalized persuasion tailoring persuasive appeals to recipients' personality traits. *Psychological Science*, *23*(6), 578–581.

Ho, S. Y., & Bodoff, D. (2014). The effects of web personalization on user attitude and behavior: An integration of the elaboration likelihood model and consumer search theory. *MIS Quarterly*, *38*(2), 497–520.

Hsieh, J. J. P.-A., Rai, A., & Keil, M. (2008). Understanding digital inequality: Comparing continued use behavioral models of the socio-economically advantaged and disadvantaged'. *MIS Quarterly*, *32*(1), 97–126.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–659.

Johnston, A. C., McBride, M., Carter, L., & Warkentin, M. (2016). Dispositional and situational factors: Influences on IS security policy violations. *European Journal of Information Systems*, *25*(3), 231–251.

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.

Jones, C., & Livne-Tarandach, R. (2008). Designing a frame: Rhetorical strategies of architects. *Journal of Organizational Behavior*, *29*(8), 1075–1099.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 518–555.

Lavine, H., Lodge, M., & Freitas, K. (2005). Threat, authoritarianism, and selective exposure to information. *Political Psychology*, *26*(2), 219–244.

Lavine, H., & Snyder, M. (1996). Cognitive processing and the functional matching effect in persuasion: The mediating role of subjective perceptions of message quality. *Journal of Experimental Social Psychology*, *32*(6), 580–604.

Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel Psychology*, *28*(4), 563–575.

Lee, T.-F., Chang, I.-P., Lin, T.-H., & Wang, C.-C. (2013). A secure and efficient password-based user authentication scheme using smart cards for the integrated EPR information system. *Journal of Medical Systems*, *37*(3), 1–7.

Levin, I. P., Schneider, S. L., & Gaeth, G. J. (1998). All frames are not created equal: A typology and critical analysis of framing effects. *Organizational Behavior and Human Decision Processes*, *76*(2), 149–188.

Liang, N., Biros, D. P., & Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems*, *33*(2), 361–392.

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J. L., & Wells, T. (2012). Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. *Journal of the American Society for Information Science and Technology*, *63*(4), 755–766.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293–334.

Mael, F., & Ashforth, B. E. (1992). Alumni and their alma mater: A partial test of the reformulated model of organizational identification. *Journal of Organizational Behavior*, *13*(2), 103–123.

Maheswaran, D., & Chaiken, S. (1991). Promoting systematic processing in low-motivation settings: Effect of incongruent information on processing and judgment. *Journal of Personality and Social Psychology*, *61*(1), 13.

Mahoney, K. T., Buboltz, W., Levin, I. P., Doverspike, D., & Svyantek, D. J. (2011). Individual differences in a within-subjects risky-choice framing study. *Personality and Individual Differences*, *51*(3), 248–257.

Maier, C., Wirth, J., Laumer, S., & Weitzel, T. (2017). Personality and Technostress: Theorizing the influence of IT mindfulness. *Proceedings of the International Conference on Information Systems*. Seoul, South Korea.

McAdams, D. P., & Pals, J. L. (2006). A new Big Five: Fundamental principles for an integrative science of personality. *American Psychologist*, *61*(3), 204.

McCrae, R. R., & Costa, Jr, P. T. (1999). A five-factor theory of personality. *Handbook of Personality: Theory and Research*, *2*, 139–153.

Meyer, J. P., Paunonen, S. V., Gellatly, I. R., Goffin, R. D., & Jackson, D. N. (1989). Organizational commitment and job performance: It's the nature of the commitment that counts. *Journal of Applied Psychology*, *74*(1), 152–156.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, *83*(2), 340–363.

Moschis, G. P. (2003). Marketing to older adults: An updated overview of present knowledge and practice. *Journal of Consumer Marketing*, *20*(6), 516–525.

Peter, J. P. (1981). Construct validity: A review of basic issues and marketing practices. *Journal of Marketing Research*, *18*(2), 133–145.

Peters, G.-J., Ruiter, R. A., & Kok, G. (2014). Threatening communication: A qualitative study of fear appeal effectiveness beliefs among intervention developers, policymakers, politicians, scientists, and advertising professionals. *International Journal of Psychology*, *49*(2), 71–79.

Petty, R. E., & Cacioppo, J. T. (1980). Effects of issue involvement on attitudes in an advertising context. *Division 33 Program of the 88th Annual Convention of the American Psychological Association*. Montreal, Canada: American Psychological Association, 75–79.

Petty, R. E., & Cacioppo, J. T. (1981). *Attitudes and persuasion: Classic and contemporary approaches*. Dubuque, IA: William C. Brown.

Petty, R. E., & Cacioppo, J. T. (1986a). The elaboration likelihood model of persuasion. In Petty, R. E. and Cacioppo, J. T. (Eds.) *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*. New York: Springer-Verlag, 1–24.

Petty, R. E., & Cacioppo, J. T. (1986b). The elaboration likelihood model of persuasion. *Advances in Experimental Social Psychology*, *19*, 123–205.

Petty, R. E., Cacioppo, J. T., & Goldman, R. (1981). Personal involvement as a determinant of argument-based persuasion. *Journal of Personality and Social Psychology*, *41*(5), 847–855.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management*, *12*(4), 531–544.

PricewaterhouseCoopers. (2017). The global state of information security survey 2017. Accessed on July 11, 2018. Available at: https://www.pwc.com/gsiss2017.

Priester, J., Wegener, D., Petty, R., & Fabrigar, L. (1999). Examining the psychological process underlying the sleeper effect: The elaboration likelihood model explanation. *Media Psychology*, *1*(1), 27–48.

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

Roberts, A. (1995). "Civic discovery" as a rhetorical strategy. *Journal of Policy Analysis and Management*, *14*(2), 291–307.

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

Schwartz, D. G., & Te'eni, D. (2000). Tying knowledge to action with kMail. *IEEE Intelligent Systems and Their Applications*, *15*(3), 33–39.

Scott, J. (1991). The measurement of information systems effectiveness: Evaluating a measurement instrument. *Fifteenth International Conference on Information Systems*. Vancouver, BC.

Simon, H. A. (1979). Rational decision making in business organizations. *The American Economic Review*, *69*(4), 493–513.

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

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee systems security policy violations. *MIS Quarterly*, *34*(3), 487–502.

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.

Steenkamp, J. B. E. M., & Baumgartner, H. (1998). Assessing measurement invariance in cross-national consumer research. *Journal of Consumer Research*, *25*(1), 78–93.

Straub, D. W. (2009). Black hat, white hat studies in information security, Keynote Address. *International Federation for Information Processing (IFIP) WG8.11/11.13 Workshop*. Cape Town, South Africa.

Suddaby, R., & Greenwood, R. (2005). Rhetorical strategies of legitimacy. *Administrative Science Quarterly*, *50*(1), 35–67.

Tajfel, H. (1978). The achievement of group differentiation. In H. Tajfel (Ed.), *Differentiation between social groups: Studies in the social psychology of intergroup relations*. London: Academic Press, 77–96.

Tajfel, H. (1981). *Human groups and social categories: Studies in social psychology*. Cambridge: Cambridge University Press.

Tajfel, H. (1982). *Social identity and intergroup relations*. Cambridge, England: Cambridge University Press.

Tajfel, H., & Turner, J. (1985). The social identity theory of intergroup behavior. In S. Worchel & W. G. Austin (Eds.), *Psychology of intergroup relations*. Chicago: Nelson-Hall, 7–24.

Tam, K. Y., & Ho, S. Y. (2005). Web personalization as a persuasion strategy: An elaboration likelihood model perspective. *Information Systems Research*, *16*(3), 271–291.

Tanner, J. F., Hunt, J. B., & Eppright, D. R. (1991). The protection motivation model: A normative model of fear appeals. *Journal of Marketing*, *55*(3), 36–45.

Taylor, S. E. (1981). The interface of cognitive and social psychology. *Cognition, social behavior, and the environment*, 189–211.

Te'eni, D. (2001). Review: A cognitive-affective model of organizational communication for designing IT. *MIS Quarterly*, *25*(2), 251–312.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3), 190–198.

Wan, E. W., & Rucker, D. D. (2013). Confidence and construal framing: When confidence increases versus decreases information processing. *Journal of Consumer Research*, *39*(5), 977–992.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). Then influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, *20*(3), 267–284.

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

Williams, K. C. (2012). Fear appeal theory. *Research in Business Economics Journal*, *5*(1), 1–21.

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

Witte, K., Cameron, K. A., McKeon, J. K., & Berkowitz, J. M. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, *1*(4), 317–341.

Witte, K., Meyer, G., & Martell, D. (2001). *Effective health risk messages: A step-by-step guide*. Thousand Oaks, CA: Sage Publications.

Yalch, R. F., & Elmore-Yalch, R. (1984). The effect of numbers on the route to persuasion. *Journal of Consumer Research*, *11*(1), 522–527.

Yu, N., & Shen, F. (2013). Benefits for me or risks for others: A cross-culture investigation of the effects of message frames and cultural appeals. *Health Communication*, *28*(2), 133–145.

APPENDIX A

Fear Appeals Used in the Experiment (Followed Informed Consent and Instructions)

Individually Focused Fear Appeal (Designed to Align with Employees with Low Organizational Identification)

There have been frequent recent reports of increased threats to individual computer systems and personal data kept on the network. Your computer may be under attack by individuals and software designed to capture the passwords you use to log onto the network. Hackers can now use various technologies and techniques to capture or guess your password so that they can gain access to your personal sensitive files.

Changing your password more frequently is an easy and inexpensive way to counter this threat and protect your personal computer and your personal data. Another way is to choose a "strong" password of at least eight characters that include letters, numbers, and special characters. These are effective ways to protect your sensitive data.

It is recommended that you change your password this week, and remember to change it frequently. Further information about password protection is available on the *** IT website.

Organizationally Focused Fear Appeal (Designed to Align with Employees with High Organizational Identification)

There have been frequent recent reports of increased threats to our computer systems and to the data kept on the *** network. Our computer systems may be under attack by individuals and software designed to capture the passwords used to log onto the *** network. Hackers can now use various technologies and techniques to capture or guess our passwords so that they can gain access to our sensitive *** files.

Changing passwords more frequently is an easy and inexpensive way for us to counter this threat and protect *** computer systems and data. Another way is for all *** employees and students to choose a "strong" password of at least eight characters that include letters, numbers, and special characters. These are effective ways for us to protect ***'s sensitive data.

It is recommended that all *** employees and students change their passwords this week, and remember to change them frequently. Further information about password protection is available on the *** IT website.

Note: The organization's normal acronym has been replaced with "***" here to maintain the anonymity of the review process.

APPENDIX B

Manipulation Check (Following the Fear Appeal Manipulation in Appendix A)

A manipulation check was performed to determine whether the participants perceived the message to have a high or low organizational identification orientation. Each participant was asked to rate the message in terms of the degree to which they perceived the message as orientated to the organization. The response was measured on a Likert scale ranging from low (0) to high (5). As can be seen from the results provided in Table B1, an Analysis of Variance (ANOVA) test indicated significance differences in the participants' perceptions. The messages designed to have an organizational argument rhetoric were perceived to have a higher organizational orientation than messages designed to have an individual argument rhetoric.

Table B1: Manipulation check results.

	Individually Focused Message		Organizationally Focused Message		ANOVA	
	Mean	Std dev	Mean	Std dev	*F*-test	Significance
Degree of organizational orientation	2.099	1.380	3.677	.9541	3.527	$p < .01$

APPENDIX C

Scales and Instrument Items (Following the Fear Appeal Manipulation)

For the following scales utilized in this study, the participants were asked to select a single score from 1 to 5 where, 1 means you strongly disagree with the statement, and 5 means you strongly agree with the statement. Note that these items followed exposure to one of the two fear appeals (our treatments), and these items were followed by the opportunity to proceed to change their password now (behavior).

General Purpose (for general screening purposes)

(1) I maintain important data on a specific computer or device
(2) I am responsible for the detection, prevention, and/or removal of threats to that data
(3) I am concerned for the protection of the data on that computer

Organizational Identification

(1) When someone criticizes this organization, it feels like a personal insult (OGID1)
(2) I am very interested in what others think about this organization (OGID2)
(3) When I talk about this organization, I usually say "we" rather than "they" (OGID3)
(4) This organization's successes are my successes (OGID4)
(5) When someone praises this organization, it feels like a personal compliment (OGID5)
(6) If a story in the media criticized this organization, I would feel embarrassed (OGID6)

Password Threat Severity

(1) If my password was stolen, the consequences would be severe (TSEV1)
(2) If my password was stolen, the consequences would be serious (TSEV2)
(3) If my password was stolen, the consequences would be significant (TSEV3)

Password Threat Susceptibility

(1) My password is at risk of being stolen (TSUS1)
(2) It is likely that my password will be stolen (TSUS2)
(3) It is possible that my password will be stolen (TSUS3)

Self-Efficacy

(1) Changing my password is easy to do (SEFF1)
(2) Changing my password is convenient to do (SEFF2)
(3) I am able to change my password without much effort (SEFF3)

Response Efficacy

(1) Changing my password works for protection (RESP1)

(2) Changing my password is effective for protection (RESP2)

(3) By changing my password, my password is more likely to be protected (RESP3)

Response Costs

(1) Changing my password would be time consuming (COST1)

(2) Changing my password would take work time (COST2)

(3) Changing my password would make my life more difficult (COST3)

(4) Changing my password inconveniences my work (COST4)

(5) Changing my password would require a considerable investment of effort other than time (COST5)

(6) There is too much overhead associated with the changing of passwords (COST6)

Behavioral Intent

(1) I intend to change my password within the next week (BINT1)

(2) I predict I will change my password within the next week (BINT2)

(3) I plan to change my password within the next week (BINT3)

Allen C. Johnston is an Associate Professor of Management Information Systems in the Department of Information Systems, Statistics, and Management Science within the Culverhouse College of Commerce at the University of Alabama. The primary focus of his research is in the areas of innovation, behavioral information security, privacy, data loss prevention, and collective security and his research can be found in such outlets as *MIS Quarterly, Journal of the AIS, European Journal of Information Systems, Information Systems Journal, Communications of the ACM, Journal of Organizational and End User Computing, Information Technology and People,* and *The 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).

Merrill Warkentin is the James J. Rouse Professor of Information Systems in the College of Business at Mississippi State University. His primary research focus is in behavioral IS security and privacy issues, and has appeared in *MIS Quarterly*, *Decision Sciences*, *Journal of MIS*, *Journal of the AIS*, *European Journal of Information Systems*, *Information Systems Journal, Decision Support Systems*, *Information & Management,* and others. He was the 2016 AMCIS Program Co-Chair. He holds or has held editorial positions at *MIS Quarterly*, *Information Systems*

Research, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Decision Sciences*, *and Information & Management*.

Alan R. Dennis is Professor of Information Systems and holds the John T. Chambers Chair of Internet Systems in the Kelley School of Business at Indiana University. He was named a *Fellow of the Association for Information Systems* in 2012. Prof. Dennis has written more than 150 research papers, and has won numerous awards for his theoretical and applied research. His research focuses on three main themes: team collaboration; IT for the subconscious; and digital innovation. He is Editor-in-Chief of *AIS Transactions on Replication Research* and Vice President for Conferences for the Association for Information Systems. Prof. Dennis has also written four books (two on data communications and networking, and two on systems analysis and design).

Mikko Siponen is full professor of Information Systems. He has served 10 years as a Head of Department, vice head or a director of a research center. His degrees include Doctor of Social Sciences, majoring in Philosophy; MSc in Software Engineering; Lic Phil in Information Systems; and PhD in Information Systems. He has received over 10 million EUR of research funding from corporations and numerous other funding bodies. Besides leading industry-funded projects, Siponen has been a PI on projects for the Academy of Finland, the EU, and the Finnish Funding Agency for Innovation. He has published more than 50 articles in journals such as *MIS Quarterly, Information Systems Research, Journal of the Association for Information Systems,* and *Journal of Management Information Systems*.