MIS Quarterly

RESEARCH ARTICLE

AN ENHANCED FEAR APPEAL RHETORICAL FRAMEWORK: LEVERAGING THREATS TO THE HUMAN ASSET THROUGH SANCTIONING RHETORIC[1]

Allen C. Johnston
Department of Management and Information Systems, Collat School of Business, University of Alabama Birmingham,
Birmingham, AL 35294-4460 U.S.A. {ajohnston@uab.edu}

Merrill Warkentin
Department of Management & Information Systems, College of Business, Mississippi State University,
Mississippi State, MS 39762-9581 U.S.A. {mwarkentin@acm.org}

Mikko Siponen
Department of Computer Science and Information Systems, University of Jyväskylä,
FI-40014 Jyväskylä FINLAND {mikko.t.siponen@jyu.fi}

Fear appeals, which are used widely in information security campaigns, have become common tools in motivating individual compliance with information security policies and procedures. However, empirical assessments of the effectiveness of fear appeals have yielded mixed results, leading IS security scholars and practitioners to question the validity of the conventional fear appeal framework and the manner in which fear appeal behavioral modeling theories, such as protection motivation theory (PMT), have been applied to the study of information security phenomena. We contend that the conventional fear appeal rhetorical framework is inadequate when used in the context of information security threat warnings and that its primary behavioral modeling theory, PMT, has been misspecified in the extant information security research. Based on these arguments, we propose an enhanced fear appeal rhetorical framework that leverages sanctioning rhetoric as a secondary vector of threats to the human asset, thereby adding the dimension of personal-relevance threat, which is critically absent from previous fear appeal frameworks and PMT-grounded security studies. Following a hypothetical scenario research approach involving the employees of a Finnish city government, we validate the efficacy of the enhanced fear appeal framework and determine that informal sanction rhetoric effectively enhances conventional fear appeals, thus providing a significant positive influence on compliance intentions.

Keywords: Fear appeals, protection motivation theory, deterrence theory, information security, threats, responses, sanctions, rhetoric

[1] Viswanath Venkatesh was the accepting senior editor for this paper.

The appendices for this paper are located in the "Online Supplements" section of the *MIS Quarterly*'s website (http://www.misq.org).

Introduction

Information security managers and other organizational executives continue to struggle with enforcing policies designed to protect assets from intentional or accidental information security violations by an organization's insiders (D'Arcy et al. 2009; Ng et al. 2009; Puhakainen and Siponen 2010). Recent reports suggest that insider abuse ranks second only to virus incidents as the most frequent form of security breach (Richardson 2008). Recent industry surveys also indicate that over 40 percent of data breaches are attributed to negligent insiders who fail to follow policies (Ponemon Institute 2012; Wall 2011). Organizational insiders are individuals with access to organizational assets as a routine part of their responsibilities (Shaw et al. 1998). In an effort to enforce policy and to gain compliance among these insiders, security managers utilize a variety of techniques, including security education, training, and awareness (SETA) programs and events, incentive programs, and campaigns. The common denominator of all these programs is communication, that is, the manner in which managers articulate their goals and expectations to comply with information security behavior. To establish effective information security learning environments and secure organizational cultures, the effective communication of policy to all insiders is imperative (Siponen 2000). Toward achieving this goal, fear-based messages have received increasing attention from information security scholars in the effort to persuade insiders to comply with recommended security behaviors, such as those stipulated in information security policies (Herath and Rao 2009; Johnston and Warkentin 2010; Sasse et al. 2001; Weirich and Sasse 2001).

For several decades, the research of fear appeals has painted a cloudy picture of uncertainty, debate, and general disenchantment regarding the effectiveness of fear appeals (Morales et al. 2012). On the one hand, a statement issued by the Center for Substance Abuse Prevention (2012), which stated "messages that do more harm than good—e.g., 'scare tactics'—should be avoided," illustrates the disillusionment of practitioners in fear appeal usage, no doubt in response to frustrations with countless failures to achieve desired outcomes from their application (Hornik et al. 2008). On the other hand, sources such as the European Union's Analysis of the Science and Policy for European Control of Tobacco (ASPECT) consortium cited fear as an effective leverage point in enhancing the effectiveness of communication (ASPECT Consortium 2004). However, positive inferences to fear appeal usage typically stop short of prescriptions for effective use.

Scholars are seemingly attuned to the debate but have made only marginal progress in advancing our understanding of how fear appeals are experienced and can be refined to improve their effectiveness (Hastings et al. 2004; Morales et al. 2012). As Peters, Ruiter, and Kok (2013) pointed out, fear appeals have been used for years in a number of contexts, but communicators have not developed a precise formula for obtaining consistently successful results. If we seek to apply fear appeals effectively within our organizations to motivate policy compliance behaviors, the contemporary wisdom of fear appeal composition and theory must be reconsidered.

Fear appeals take the form of messages or communications intended as a mechanism for manipulating the recipient's intrinsic notions of threat and efficacy regarding a particular threat and corresponding protective behavior. Initially applied almost exclusively within the healthcare domain, early fear-inducing messages concerned health or safety-related threats (Bartholomew et al. 2011; Milne et al. 2006) to the physical self, such as injury caused by not wearing a seat belt or cancer caused by overexposure to the sun or toxic smoke inhalation. Threats of this nature are universally personally relevant because they represent threats to the self (i.e., the human asset). On the other hand, in the information security literature, the rhetoric embedded in fear appeals is typically focused on threats to the individual's things (the information assets) (Johnston and Warkentin 2010; Liang and Xue 2010). Unfortunately, the degree to which an individual perceives information assets as personally relevant is highly subjective, thus potentially marginalizing the impact of the fear appeal. These threats, while very real, are not universally personally relevant.

We contend that the conventional fear appeal rhetorical framework is inadequate in providing threat warnings when it is used in the information security context. We also contend that the primary behavioral modeling theory on which it is based, protection motivation theory (PMT), has been improperly applied in the extant information security literature (Truex et al. 2006; Weber 2012). To appeal to the self-interest of their audience, fear appeals must achieve a sufficient level of personal relevance (or issue involvement) for the individual; otherwise, they are ignored and rendered ineffective (Burnkrant and Unnava 1989; Petty and Cacioppo 1986). However, instead of being focused on threats to the physical self, such as in healthcare contexts, fear appeals in the information security context have been mostly focused on threats to the individual's things (e.g., data, information, and systems) and are vulnerable to the lack of perceived relevance. To this extent, the conventional fear appeal rhetorical framework is inadequate and requires revision.

In modeling the effect of fear appeals, PMT (Rogers 1975, 1983) supports the cognitive assessment of threats, thereby underscoring the notion that individuals will take calculated actions to protect their self-interests in avoiding the pain associated with the threats. However, as fear appeals and PMT have been applied by IS scholars for use within the information security context, two important problems have surfaced. First, PMT is a *theory of behavior change* (Velicer and Prochaska 2008). It is intended to model outcomes resulting from (and subsequent to) some type of stimulus (e.g., a fear appeal) that communicates a threat and a recommended response to the threat. However, its primary use in the information security literature has been as a *theory of behavior*. Hence, it has been used simply to understand how individuals perceive an existing threat without concern for a particular behavioral change mechanism (Anderson and Agarwal 2010; Herath and Rao 2009; Lee 2011). We will argue that this represents a misuse of the reference theory. Second, PMT does not account for subtlety in the nature of the threat; it presumes that all threats are personally relevant to the message recipient. However, IS scholars have seemingly made repeated assumptions to the contrary, which has led to a variety of compromised threat perspectives within their respective studies (Bélanger and Crossler 2011; Crossler 2010; Johnston and Warkentin 2010; Woon et al. 2005). This misspecification of the theory also presents a significant problem for information security scholars and practitioners.

In this study, we address the inadequacy of the fear appeal rhetorical framework and the problems raised by the misappropriation of PMT. Regarding the misuse of PMT's history in the literature, we offer a warning and echo Truex et al.'s (2006) call for more careful consideration of the appropriate application of PMT as a behavioral change theory. Regarding the inadequacy of the fear appeal rhetorical framework and the misspecification of PMT, however, we offer an enhanced fear appeal rhetorical framework. Our enhanced framework is created through the addition of sanctioning rhetoric to the conventional fear appeal language. Sanctions are representative of a secondary threat vector and serve as an additional source of extrinsic influence in engaging in protective behaviors that secure the employee's status in the organization. Threats, such as password theft and data loss, are threats to an organization's information assets (and thus may lack personal relevance), whereas sanctions are threats to the individual human asset because they jeopardize the employee's status or employment security. Because we apply fear appeals within a controlled organizational setting, we have the opportunity to leverage both the information *and* human asset threat vectors, thereby adding personal relevance to the threat equation and solving the problems created by the misspecification of PMT in the information security literature.

To achieve this goal, we explore the effectiveness of an enhanced fear appeal rhetorical framework through the use of a hypothetical scenario research design involving three unique threat/behavior pairs that are typical of fear appeal implementations in practice. By utilizing the predominant model for representing the impact of fear appeal and sanction elements on information security policy compliance intentions, we demonstrate that the inclusion of sanction elements in a conventional fear appeal elicits a compliance response significantly greater than that produced by contemporary usage of fear appeals.

Theoretical Background

In this section, we present a review of the rhetorical composition of fear appeals and their associated behavioral modeling theories. We then discuss the rationale for an enhanced fear appeal rhetorical framework through the addition of sanctioning rhetoric.

Fear Appeal Rhetorical Composition

Fear appeals, otherwise known as threat appeals or fear-inducing communications, can be defined either by the content of their message or by the response they engender from their target audience (O'Keefe 1990). In discussing the influence of fear appeals in modifying attitudes and behavioral intentions toward compliance with information security policies and procedures, as well as the potential interaction of sanction elements placed within the message, it is important to define clearly all the elements of a fear appeal. The primary constructs of perceived threat and perceived efficacy are firmly established in the fear appeal literature (Peters et al. 2013; Witte 1992, 1994b).

As defined by Witte (1992), a threat is an external stimulus variable that exists whether it is perceived by an individual or not. If an individual perceives a threat, he or she can be described as being aware of a threat. A properly constructed fear appeal not only serves to induce the awareness that a threat exists but also purveys the severity of the threat and its target population's susceptibility to the threat. In this message, an individual is able to formulate the perceived severity of the threat and the perceived susceptibility to the threat. In other words, once an individual is conscious of a threat, he or she will establish beliefs about the seriousness of the threat and the probability of experiencing it.

A fear appeal also contains arguments that cause an individual to form cognitions of efficacy. This perception of efficacy includes thoughts of the efficacy of the recommended response and the efficacy of the individual performing the response (Witte 1994b). Response efficacy is the degree to which an individual believes the response to be effective in alleviating a threat. Self-efficacy is the degree to which an individual believes in his or her ability to enact the recommended response (Rogers 1983; Witte 1994a).

Maddux and Rogers' (1983) addition of self-efficacy marks the last time that an element was widely accepted as an essential element of the rhetorical construction of a fear appeal. When applied in healthcare and campaigns for the awareness of threats to public safety, the conventional rhetorical construction has not been seen as a limitation. In these contexts, the threats are most often to the individual but have universal relevance. We contend, however, that this conventional rhetorical construction is inadequate in contexts where the threats are not necessarily universally personally relevant, such as information security. For this reason, we propose an enhanced rhetorical framework that resolves both this inadequacy and the associated misspecification of fear appeal behavioral models (i.e., PMT), which is described next.

Fear Appeal Behavioral Modeling Theories

Our model of the impact of fear appeals is based on the early works of Janis and Feshbach (1953), in which fear appeal strength was correlated with teeth-brushing compliance. Table 1 lists some of the most noteworthy modeling studies, including their significance and theoretical advancement. Our understanding of the impact of fear appeals has been shaped by studies that have modeled a curvilinear relationship between fear appeal strength and attitude change (e.g., Janis 1967; Liang and Xue 2010) as well as those which have suggested a linear relationship (Rogers 1975). Witte (1998) contended that these early works, in conjunction with the works of Leventhal (1970, 1971), provided a necessary progression from which contemporary behavioral models were derived. The stage model of fear-arousing communications processing by de Hoog et al. (2007) represents the most recent behavioral model, although it is not as entrenched in the literature as some earlier models are.

The majority of research on fear appeal influence modeling was conducted prior to the emergence of dual process theories of attitude and behavioral change (de Hoog et al. 2005). As described by de Hoog et al. (2005), this initial research was guided by reinforcement theory in which Hovland, Janis, and Kelly's (1953) fear-as-acquired drive model dominated. Leventhal's (1970, 1971) parallel process model set the stage for contemporary cognitive theories, such as Roger's (1975, 1983) protection motivation theory, Witte's (1992) extended parallel process model, and de Hoog et al.'s (2005) stage model of fear-arousing communications processing.

The most prevalent theory used to model the influence of a fear appeal on information security behavioral outcomes has been the PMT (Rogers 1975). PMT is decades old and has been adapted numerous times in attempts to predict security policy compliance attitudes (Herath and Rao 2009; Ifinedo 2012; Johnston and Warkentin 2010), intentions to engage in protective behavior through the adoption of protective software (Lee 2011; Lee et al. 2009; Liang et al. 2009, 2010), or other prescribed protective acts. In each of these studies, the depicted threat vector concerned the information asset, requiring the individual to assess the severity and certainty of its impact on data, systems, or any medium in which information was contained or in transit. In many cases, one or both of these threat dimensions was determined to be nonsignificant in contributing to the formulation of a response (Bélanger and Crossler 2011; Crossler 2010; Herath and Rao 2009; Johnston and Warkentin 2010; Woon 2005).

We contend that the historically poor or, at best, inconsistent outcomes of the application of PMT to information security phenomena were because of theory misuse and misspecification. Researchers in the IS discipline have often looked to other disciplines for theories that can help explain or predict IS phenomena. However, the process by which the theories have been applied to the discipline has drawn recent criticism (Avgerou 2013; Grover et al. 2008; Oswick et al. 2011; Truex et al. 2006). For example, Truex et al. (2006) argued that the theories of referent disciplines applied to IS phenomena often lack fit to the phenomena because they are adopted with little regard to the underlying assumptions or boundary conditions that constrain them to a particular phenomenon or context. Furthermore, the inattention to these assumptions has jeopardized future scholarship. Oswick et al. (2011) and Avgerou (2013) echoed this sentiment, suggesting that the theories of referent disciplines have been "domesticated" to fit IS phenomena without the rigor necessary to understand the nuances of the original theory. PMT has suffered a similar fate in its application to information security phenomena.

A critical flaw in the application of PMT in information security research has been the assumption that PMT accounts for nuances in perceptions of threat; however, it does not. PMT has been widely applied in the study of individual protective behaviors adopted by information users (Anderson and Agarwal 2010; Herath and Rao 2009; Lee and Larsen 2009; Liang and Xue 2009, 2010). The results from each application of PMT have been widely divergent, and different studies have yielded contradictory findings. One rationale for the disparity of outcomes is that scholars have applied PMT to understand the influence of fear appeals that are used to warn of information security threats without giving much

Table 1. Fear Appeal Research, Significance and Theoretical Advancement

Research	Significance	Theoretical Advancement
Hovland, Janis, and Kelly (1953)	investigated factors which determine the effectiveness of fear appeals	fear-as-acquired model (drive model)
Janis (1967)	described an inverted U-shaped relationship between fear and message acceptance	fear-as-acquired model (drive model)
McGuire (1968)	described a two factor (cues and fear) theory to explain an inverted U-shaped relationship between fear arousal and attitude change	fear-as-acquired model (drive model)
Leventhal (1970, 1971)	distinguished between cognitive and emotional appraisals of fear appeals	parallel process model
Rogers (1975, 1983)	specified perceived susceptibility, perceived severity, and response efficacy as components of a fear appeal	protection motivation theory
Maddux and Rogers (1983)	added a fourth component, self- efficacy, to fear appeal composition	protection motivation theory
Witte (1992)	extended the parallel process model by describing cognitive and emotional appraisals as sequential processes and established the role of fear as an indirect motivator of behavioral change	extended parallel process model
de Hoog, Stroebe, and de Wit (2005)	specifies the cognitive processes leading to persuasion, proposes that threat-induced defensive processes contribute to message effectiveness, and predicts differences in attitude based on threat severity and susceptibility manipulations	stage model of fear-arousing communications processing

thought to the underlying assumption of fear appeals that the threats in the fear appeals must have personal relevance (Slater 2006). However, threats to data, information, and systems do not carry the same personal relevance as threats that directly impact one's self, which is common in fear appeal applications in healthcare (Crossler 2010; Ifinedo 2012; Johnston and Warkentin 2010). By overlooking the critical underlying assumption of the threat dimension of fear appeals, researchers have misspecified the theory within the information security context (Comello et al. 2011; Slater 2006).

Nevertheless, fear appeals or PMT should not be avoided in the information security context. Fear appeals are a necessary component of a holistic security management program because threats to information assets are prevalent and must be warned against. However, the absence of rhetoric that describes threats of a personal nature jeopardizes their success. We contend that the inclusion of a secondary threat vector of threats to the human asset, that is, those responsible for performing the protective behavior, would effectively enhance the fear appeal message without fundamentally changing the purpose of the fear appeal or violating the understanding of how humans cognitively assess potentially threatening messages. However, as we add sanctioning rhetoric to this effect, we extend PMT's reach in describing the influence of the appeal. We now have additional rhetoric that requires two theories to describe its impact. One theory addresses the threat to the information asset, whereas the other theory addresses the threat to the human asset. This purposeful juxtaposition of theories allows us to account for differences in the types of threats needed to persuade insiders faced with information security threats, thereby overcoming the inadequacy of fear appeals and problems caused by the misspecification of PMT.

The Enhanced Fear Appeal Framework: Adding Sanctioning Rhetoric to Account for the Threats to the Human Asset

The extant fear appeal research points to numerous extra-message factors and human dispositions that add variability to the manner in which fear appeals are received and interpreted. These sources of influence include message completeness (Dutta and Vanacker 2000), message format (Keller and Block 1996), and personal relevance (Burnkrant and Unnava

1989), to name a few. The literature suggests that fear appeal effectiveness is partly dependent upon the design of the message and the audience for which it is intended (Burnkrant and Unnava 1989; Petty and Cacioppo 1986). The literature also contends that individuals cognitively assess the threats described in the messages and formulate response intentions based on a hedonistic, self-interest in pain avoidance (Angst and Agarwal 2009). Accordingly, the effectiveness of a fear appeal that describes a threat to an information asset is limited to the extent to which its audience associates pain with information defacement, theft, or loss, or with a security policy violation. For those with a lesser sense of data ownership or security interests, a more robust message is required, such as one that highlights a threat to which they are not immune.

Pain avoidance is also a fundamental principle of deterrence theory, which can be traced back to Jeremy Bentham (1748-1832) and Cesare Beccaria (1738-1794). Deterrence theory suggests that individuals choose to commit a crime if the benefits outweigh the risks. Specifically, deterrence theory suggests that if an individual believes that the risk of getting caught is high (certainty of sanctions), that severe penalties will be applied if one is caught (severity of sanctions), and that punishment will be swift (celerity of sanctions), then the individual is less motivated to commit a crime or engage in rule-breaking behavior. Although the original deterrence theory focused on formal sanctions, research during the last few decades has added the "non-legal costs" (Pratt and Cullen 2000, p. 367), in which informal sanctions (Piquero and Tibbetts 1996) are the most notable. A common operationalization of informal sanctions is to measure the disapproval of friends or peers regarding a given action (Paternoster and Simpson 1996), which typically leads to feelings of guilt and shame.

Deterrence theory has been widely applied in information security research, especially the role of perceived sanction severity and certainty (D'Arcy and Devaraj 2012). Straub and Nance (1990) suggested that the detection and punishment of violators minimizes computer abuse. Similarly, Straub (1990) found that the use of information security deterrents resulted in the decreased incidence of computer abuse. The following deterrents were found effective: weekly hours dedicated to IS security, use of multiple methods to disseminate information about penalties and acceptable system usage, and clear statements of penalties for violations (Straub 1990). These were found to increase the insider's risk of getting caught (certainty of sanctions) and the perception that severe sanctions would be imposed if the violator was caught (severity of sanctions). Straub and Welke (1998) carried out an action research study in which they highlighted the importance of communicating certainty and severity of sanctions, as a part of insider education and training programs, in order to minimize security violations. Following this research, Kankanhalli et al. (2003) investigated whether the use of sanctions led to enhanced IS security effectiveness and found that deterrents, as measured in man-hours spent in security efforts, led to the improved effectiveness of information security.

Straub et al. (1993) further applied deterrence theory by carrying out a field experiment that tested whether student cheating during a programming assignment could be prevented. They concluded that managers should stress that violations of an organization's information security policies would result in sanctions. Harrington (1996) found that codes of ethics, a type of formal sanction applied to the organization generically, did not affect insiders' judgments or intentions to commit computer abuse. However, generic codes of ethics were found to affect insiders who were high in the denial of responsibility, which is a form of rationalization. Similarly, IS-specific codes of ethics did not affect judgment or intentions, except in the case of computer sabotage, which is a severe type of computer abuse. Thus, the effects of codes of ethics were found to be "sporadic and weak" (Harrington 1996, p. 273). D'Arcy et al. (2009) found that IS security policies, awareness programs, and computer monitoring influenced the perceived severity of formal sanctions, which led to the reduced intention to misuse IS. In their study, the certainty of formal sanctions did not have any effect on intention to misuse IS. However, Siponen et al. (2007) applied both formal and informal sanctions in order to explain insiders' compliance with information security policies and found that both forms of sanctions predicted insiders' compliance with IS security policies. D'Arcy and Devaraj (2012) later found both forms of sanctions to have both direct and indirect influence on intentions to misuse technology.

In summary, although the results of previous studies are mixed and opinions are diverse about the definitive role of sanctions on information security compliance intentions and behaviors (D'Arcy and Herath 2011), they are representative of threats to a human asset. There is enough evidence to suggest that they have the potential to compliment the conventional information asset threat rhetoric and help form an enhanced fear appeal rhetorical framework. As shown in in Figure 1, threat assessments stemming from such a framework include the evaluations of threats to both the information asset and the human asset.

The following section presents and tests an enhanced fear appeal research model based on the framework described above. This model contains the conventional elements of a fear appeal, augmented by elements of formal and informal forms of sanction severity, sanction certainty, and sanction

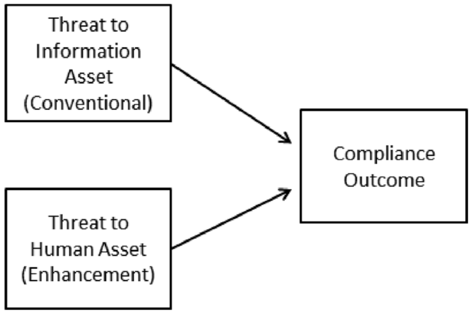

Threat to Information Asset (Conventional)
Threat to Human Asset (Enhancement)
Compliance Outcome

Figure 1. Fear Appeal Rhetorical Enhancement Conceptual Model

celerity. As described earlier, each of these elements is well established in the deterrence literature and should serve as a driver for the enhanced effectiveness of fear appeal in the form of increased information security compliance outcomes. We preface this section with the reminder that the focus of this study and its subsequent contribution is the fear appeal *mechanism*, that is, the fear appeal rhetorical framework that has remained relatively unchanged and has guided fear appeal composition since the mid-1970s. Our primary arguments are that this framework is inadequate when applied to the information security context and that its unrefined use within this context has generated inconsistent outcomes and a general misappropriation of its primary behavioral modeling theory, PMT.

Testing the Enhanced Fear Appeal Rhetorical Framework

In this study, we aim to understand how the inclusion of sanctioning rhetoric, as a secondary threat vector to human assets within a traditional fear appeal, resolves the tension in information security scholarship, which is imposed by the inadequacies of contemporary fear appeal rhetoric composition and the associated misspecification of PMT. Based on the guidance provided by the fear appeal and deterrence literature, and their respective, dominant nomological models, we have formed a juxtaposed research model. This model represents our estimation of how fear appeal rhetoric is interpreted and is able to dictate the responses of individuals faced with threats to information assets and mandated to comply with policy under the threat of sanctions to themselves. As illustrated in Figure 2, the research model incorporates the conventional rhetorical elements of a fear appeal and is enhanced by sanction celerity and both formal and informal forms of sanction certainty and sanction severity.

Impact of Formal and Informal Sanction Severity on Compliance Intention

In deterrence theory, undesirable behavior can be deterred by the communication of absolute, swift, and severe sanctions (Akers 1990; Williams and Hawkins 1986). Although recent research on deterrence theory has revealed inconsistencies in explaining the effects of sanctions on security behavioral intentions (Herath and Rao 2009; Kankanhalli et al. 2003; Pahnila et al. 2007), the theory has largely been well received within the behavioral information security research community and remains viable for modeling the effects of deterrence elements in the formulation of compliance attitudes (Kankanhalli et al. 2003), assuming these elements are applied in a manner consistent with the theory's underlying assumptions.

A potential recourse for the continuation of deterrence theory as a legitimate theory used to explain and predict policy compliance intentions is through the added granularity of deterrence constructs. Formal and informal sanctions are differentiated in IS and criminology research, as are sanction severity, sanction certainty, and sanction celerity. Missing in the deterrence theory literature and its application in the domain of IS research and information security studies is the extra level of granularity gained by distinguishing between formal and informal varieties of sanction severity and certainty. However, because previous research provides no direct support for the distinct roles of formal and informal sanctions in the compliance intentions of insiders, we must form our expectations of compliance intentions from the collective, indirect evidence provided by studies that broadly inspect the relative influence of formal and informal sanctions on employee compliance (Hollinger and Clark 1982; Siponen and Vance al. 2010; Li et al. 2014).

In this study, sanction severity is defined as the degree to which sanctions in response to violations of information secu-

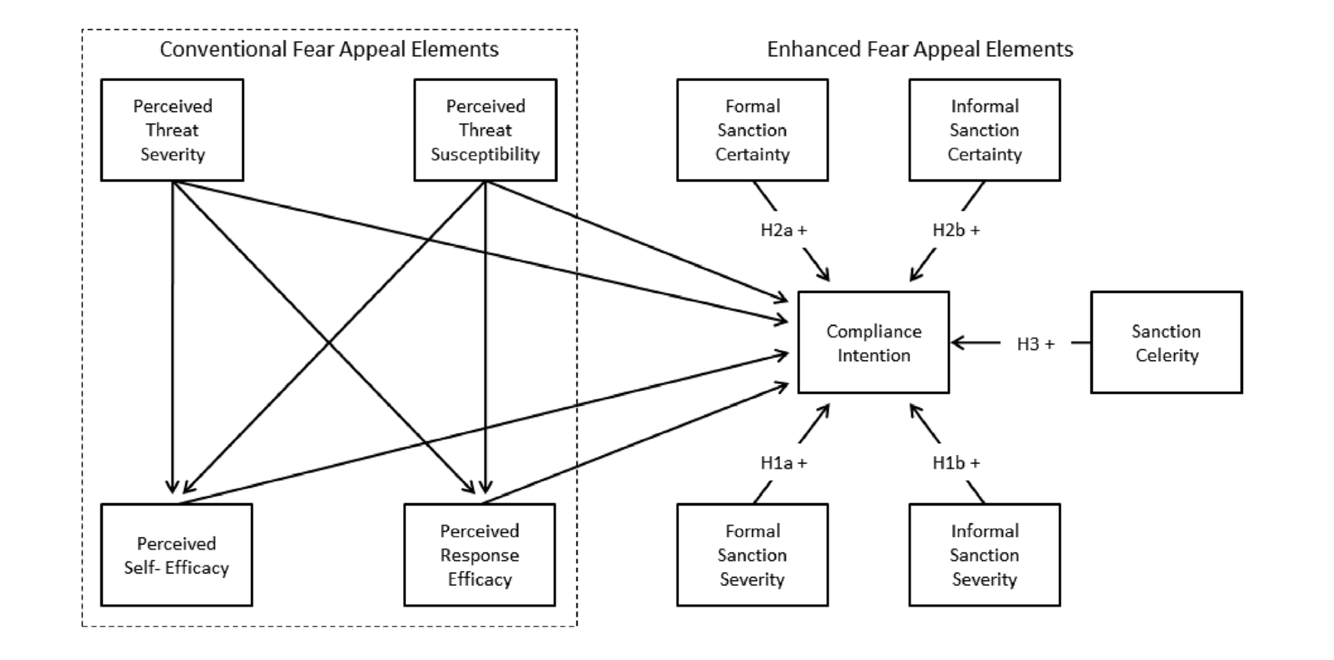

Conventional Fear Appeal Elements
Enhanced Fear Appeal Elements
Perceived Threat Severity
Perceived Threat Susceptibility
Formal Sanction Certainty
Informal Sanction Certainty
H2a +
H2b +
Compliance Intention
H3 +
Sanction Celerity
H1a +
H1b +
Perceived Self- Efficacy
Perceived Response Efficacy
Formal Sanction Severity
Informal Sanction Severity

Figure 2. Research Model for Testing the Enhanced Fear Appeal Rhetorical Framework

rity policies are perceived as harsh or problematic, while sanction certainty is defined as the degree to which the sanctions are perceived as inevitable or expected (D'Arcy et al. 2009; Straub 1990). Sanction celerity is defined as the perceived promptness with which sanctions follow the violation of the policies. The underlying assumptions of deterrence theory specify that when an individual contemplates the violation of a social norm or an established rule, this person will consider the impact of expected sanctions in terms of their severity, certainty, and timeliness. If the sanctions are provided by an authoritative source, the severity, certainty, and celerity characteristics of the sanctions will influence how the individual contemplates the violation.

Although deterrence theory originated within the criminology literature as a theory for understanding criminal and deviant behaviors, its assumptions are valid in the organizational context and to the study of security policy compliance perceptions and outcomes. Within the context of information security policy compliance, when an insider considers violating an information security policy, he or she will not only consider the severity of any pending punishment, but will also consider the likelihood that the penalty will be enforced and any latency that may occur before the penalty is handed down. The severity and certainty of formal sanctions refers to the harshness and inevitableness, respectively, of the penalties enforced by the organization. These sanctions may be in the form of formal reprimands, such as leave without pay or a demotion in rank. Alternatively, informal sanction severity and certainty refer to the harshness and inevitableness, respectively, of penalties imposed by friends or a peer group because of information security policy violations. Sanctions of this type may be in the form of social ostracization or diminished social capital. In many instances, both forms of sanctions (formal and informal), and their severity, certainty, and celerity characteristics, will be brought to bear on shaping an insider's information security policy violation intentions, just as they are in formulating deviant behavior intentions among citizens governed by laws and social norms.

Numerous information security studies have examined sanction severity as a distinct dimension of deterrence and have applied this distinction toward understanding the intentions of employees to comply with security policies. For instance, D'Arcy et al. (2009) provided direct support for the positive influence of sanction severity on deterring employee misbehavior. Herath and Rao (2009) also found that sanction severity positively influenced policy compliance intentions. Both of these studies successfully contextualized sanction severity from the criminology literature to the study of organizational policy compliance, providing footing for future studies to leverage deterrence theory for the study of policy compliance among organizational insiders. These studies did not, however, distinguish formal sanctions from informal sanctions. Although several studies distinguish between formal and informal sanctions in modeling the influence of sanctions on intentions to violate security policy, they do not differentiate between sanction severity and sanction certainty. For instance, Hollinger and Clark (1982) found both formal and informal sanctions to be positive indicators of employee conformity with management expectations. The management expectations espoused in Holliger and Clark's study are parallel to recommended protective strategies provided by management to organizational insiders. Siponen and Vance (2010) tested composite measures of formal and informal sanctions, based on a product of sanction severity and sanction certainty, and found them to be significant deterrents of policy violation intentions when techniques of neutralization were not taken into account.

Collectively, the research in these two veins of literature suggests that rhetoric describing the severity of both formal and informal sanctions will have a positive influence on an employee's intentions to engage in the recommended security activities described in a fear appeal. We draw on the work of D'Arcy et al. and of Herath and Rao to establish that sanction severity influences compliance intentions, while leveraging the work of Hollinger and Clark and of Siponen and Vance to extend this understanding and contend that formal and informal sanctions are distinct in their influence. As one contemplates whether or not to comply with recommended protective strategies, he or she will consider the severity of any possible sanctions, both of a formal nature presented by the organization and of an informal nature stemming from the actions and tone of one's peers. Such sanctions could, given the source and type of influence, indeed be different in magnitude, although the effects themselves are expected to be positive. We therefore hypothesize the following:

H1a: Rhetoric describing formal sanction severity will positively affect the intention to comply with recommended protective strategies provided by a fear appeal.

H1b: Rhetoric describing informal sanction severity will positively affect the intention to comply with the recommended protective strategies provided by a fear appeal.

Impact of Formal and Informal Sanction Certainty on Compliance Intention

Similar to the extant research involving sanction severity, no previous study has distinguished between formal and informal dimensions of sanction certainty. However, many previous studies of sanction severity also include sanction certainty as a determinant of compliance intentions, which indicates that sanction certainty serves as a positive deterrent to employee misbehavior (D'Arcy et al. 2009) and policy violation intentions (Herath and Rao 2009). Combined with our current understanding of the distinct influence provided by formal and informal sanctions (Hollinger and Clark 1982; Siponen and Vance 2010), we extend the findings of D'Arcy et al. and of Herath and Rao to expect that the certainty of formal sanctions, that is, the penalties enforced by the organization, will have a significant positive influence on an insider's intentions to comply with recommended protective actions. Similarly, we can expect that rhetoric describing the certainty of informal sanctions, that is, penalties imposed by friends or a peer group, will also have a significant impact on compliance intentions. For example, an organization's rhetoric may encourage employees to comply or require them to comply to varying degrees (e.g., "employees must comply" versus "employees failing to comply will be terminated"). Likewise, informal sanctions may also take the form of good-natured banter and teasing or extend to ostracizing. The underlying reasons and extent of impact on the outcome consequently differ. We therefore hypothesize the following:

H2a: Rhetoric describing formal sanction certainty will positively affect intention to comply with recommended protective strategies provided by a fear appeal.

H2b: Rhetoric describing informal sanction certainty will positively affect intention to comply with recommended protective strategies provided by a fear appeal.

Impact of Sanction Celerity on Compliance Intention

Several criminologists, such as Gibbs (1975) and Tittle and Rowe (1974), have voiced concerns about the relevance of sanction celerity, arguing that celerity is more relevant to animal behavior than to human behavior (Howe and Loftus 1996). Perhaps as a result, the role of celerity as a deterrent has received less attention from both criminologists and IS scholars (D'Arcy and Herath 2011). A few exceptions (Hu et al. 2011; Siponen et al. 2007) have shown celerity to be a nonsignificant determinant of deterrence behavior. In a context similar to the current study and in line with the underlying assumptions of deterrence theory, Hu et al. (2011) found no support for the influence of sanction celerity on policy violation intentions. Therefore, following Gibbs, and Tittle and Rowe, and consistent with the fact that the extant information security research has not established sanction celerity as a positive influence on intention to comply, we offer the following null hypothesis:

H3: Rhetoric describing sanction celerity will not affect intention to comply with recommended protective strategies provided by a fear appeal.

Research Design

In the empirical assessment of the research model and its associated hypotheses, we followed a sequential mixed-methods research approach that incorporated qualitative and quantitative data collection (Venkatesh et al. 2013), the latter of which involved a two-group posttest-only randomized experimental design. The qualitative data collection involved interviews with organizational leaders in the sampling frame, while in the quantitative data collection, the experimental design required two groups of randomly assigned participants, one of which received one of three fear appeal treatments followed by a survey, while the other group received only the survey. This approach has a strong tradition in IS research and provides an acceptable level of rigor for positivistic variance model analysis (Kaplan and Duchon 1988).

The sample of interest comprised the employees of multiple suborganizational offices within a city government in Finland. We also refer to these employees as insiders. These insiders perform a number of information technology (IT) related tasks on behalf of the city, supporting functional areas pertaining to social services, city sports and education, planning and construction, tourism, leisure, and city administration and economics, among others. This government office had published information security policies, along with designated IT security managers within each suborganizational office that was compelled to enforce them. Furthermore, the insiders were self-identified as directly responsible for the protection of sensitive government data. All aspects of the research design and execution, including fear appeal and survey development, were approved by the appropriate research ethics committee of the principle investigators.

Fear Appeal Design

The first stage of this research design involved a series of interviews with four organizational leaders and insiders of the city government in Finland. These interviews were intended to accomplish several goals, including the enhancement of our understanding of the context and form of the messaging typically implemented in the organization and our understanding of the type of security violations that typically occur. We also learned about the role of policy documents that support the mitigation of these violations. The results of these interviews facilitated the appropriate construction of three fear appeal messages, one for each common form of policy violation indicated by the organizational leaders. Each fear appeal message was designed to elicit a maximum range of response variance, while maintaining the level of relevance and realism necessary to warrant its sincere consideration.

One fear appeal message addressed the threat of password theft and encouraged insiders to change their password to a "strong" password of at least eight characters that included letters, numbers, and special characters. The second fear appeal message addressed universal serial bus (USB) memory card theft and encouraged insiders to protect their USB drives by encrypting the data stored on them. The third fear appeal message addressed data theft caused by not logging off or locking workstations, and it reminded insiders to log off or lock their respective systems when leaving them for any amount of time. Each fear appeal message was constructed to contain language that addressed all of the elements typically found in a fear appeal, including threat severity, threat susceptibility, response efficacy, and self-efficacy. In contrast to previous studies, we also included the elements of sanction severity, sanction certainty, and sanction celerity. Sanction certainty and sanction severity included both formal and informal dimensions[2] that were intended to articulate the threat to the human's employee status or employment security. The three fear appeals are presented in Appendix A.

Instrument Development

Following the construction of the three fear appeal messages, we designed an appropriate survey instrument with instructions and items for measuring the individual-level latent constructs adapted from previous research. The conventional fear appeal elements of threat severity, threat susceptibility, self-efficacy, and response efficacy were each measured using the three-item reflective scales first established by Witte et al. (1996) and later used successfully by Johnston and Warkentin

[2] Based on feedback from organizational leaders, formal sanctions within the organization do exist, but are tied to the severity and context of non-compliance. Therefore, to ensure content validity and relevance to the organizational environment of our subjects, we could not include explicitly stated sanctions in our fear appeals, but we could allude to the presence of both formal and informal sanctions.

(2010). The five-item reflective measure of sanction celerity and the three-item formal and informal varieties of sanction severity and sanction certainty were also adapted from previously validated instruments (Paternoster and Simpson 1996; Siponen and Vance 2010). The dependent variable, *intention to comply with recommended protective strategies*, was adapted from Johnston and Warkentin. The instrument also contained items designed to capture the demographics of our study's sample, including age, gender, work experience, and education level. All measures, with the exception of the demographic items, involved in this study were assessed using a five-point Likert-type scale that was anchored by 1 = strongly disagree, 3 = neutral, and 5 = strongly agree. The full instrument is provided in Appendix C.

Fear Appeal and Instrumentation Review and Pretest

In the next stage, an expert review panel was convened to provide additional insights and ideas that would allow for the refinement of the fear appeals and survey instrument. This panel consisted of seven faculty members and Ph.D. students at the home universities of the current study's research team. These panelists were regarded as knowledgeable in research instrument design and fear-based communication, having conducted numerous similar experimental design studies involving the measures used in this research. Additionally, we consulted three subject matter experts who are responsible for information security policy compliance in the organization from which the sample was drawn. Based on the feedback from the expert review panel, the fear appeal messages were found to be appropriate for each threat/behavior pair and were considered at a moderate level of intensity[3] in all elements of the fear appeals. The panelists also provided comments that were useful in refining the grammar and wording of the fear appeals. Finally, the full instrument was reviewed by several city government experts for relevance and their approval.

Prior to the primary data collection, the fear appeals and corresponding survey were pretested using the same distribution mechanism and survey tool used in the primary data collection. Forty individuals, who were leaders and employees of the city government and who were not interviewed in the earlier stage of this study, were solicited to participate in the study, mirroring the process that would be used in the data collection. The feedback from this group provided a degree of assurance that the data collection mechanisms functioned properly. The data collected in this pretest of the survey instrument was used for the validation of the instrument's psychometric properties (Straub 1989). The reliability of the instrument's measures was assessed using Cronbach's α, while convergent and discriminant validity was assessed using principal components analysis. The only casualties of this assessment were two items in the sanction celerity measure, which had nonsignificant loadings. The results of these assessments provided a reasonable level of assurance that the instrument's measures would yield purposeful results during the primary data collection.

Common method variance (CMV) is a bias introduced into a study when the predictor and dependent variables are collected at a single point in time from a single source. We address this bias using both a procedural and statistical approach (MacKenzie et al. 2011; Podsakoff et al. 2003). Procedurally, we take an *a priori* approach to CMV and address common method effects stemming from the source, or rater, item characteristics, and context during the scale development and evaluation. This anonymous study's scales were evaluated by the expert review panel described above and randomized upon administration. In the statistical assessment of CMV, we followed Podsakoff et al.'s (2003) recommendations by conducting a confirmatory factor analysis both with and without a single unmeasured latent method factor. The results of this analysis did not indicate a significant difference (χ^2/df = 0/1), which suggested that CMV is not a threat.

Primary Data Collection

The primary data for this study were obtained from insiders of multiple suborganizations within the same city government in Finland and used in the fear appeal design interviews and in the pretest of the survey instrument. Of the 2,475 potential insiders, 559 complete and error-free responses to our e-mail request for participation were received, resulting in a 22.6 percent response rate. Each insider was randomly assigned to one of the three fear appeal messages or to a control group that did not receive a fear appeal message. A total of 175 insiders received the password theft fear appeal, 118 received the data theft from not logging out fear appeal, and 155 received the USB theft fear appeal, while 111 received no fear appeal message of any kind. The fear appeals and subsequent survey were presented via a web-based survey tool and provided with the assurance of anonymity.

[3] Moderate levels of intensity are desirable because mildly worded appeals have insufficient impact, and very intense levels are associated with maladaptive responses to control the fear (by discounting the appeal), instead of adaptive responses to control the threat (by adopting the recommended response).

Table 2. Demographic Information for Primary Data Sample

Gender	Age*	Work Experience	Education Level*
male (count of 244; 44%) female (count of 315; 56%)	18 to 29 years (count of 47; 8.4%) 30 to 39 years (count of 111; 19.9%) 40 to 49 years (count of 181; 32.4%) 50 to 59 years (count of 184; 32.9%) over 60 years (count of 33; 5.9%)	< 6 months (count of 13; 2.3%) 6 to 12 months (count of 8; 1.4%) > 1 year to 2 years (count of 18; 3.2%) > 2 years to 3 years (count of 16; 2.9%) > 3 years (count of 503; 90%)	high school (count of 50; 8.9%) some college (count of 52; 9.3%) Bachelor's Degree (count of 148; 26.5%) Master's Degree (count of 80; 14.3%) Doctorate (count of 2; 0.4%) other (unspecified) (count of 220; 39.4%)

***Note**: Some respondents chose not to disclose age or education level.

Table 3. Descriptive Information and Results of Test of Internal Validity

	Fear Appeal						No Fear Appeal		F-test comparison of means between control group and collective fear appeal group	
	Password Theft (N = 175)		Data Theft From Not Logging Out (N = 118)		USB Theft (N = 155)		Control Group (N = 111)			
Variable	mean	std dev	mean	std dev	mean	std dev	mean	std dev	F	sig
threat severity	3.96	0.89	4.11	0.81	4.11	1.19	1.96	0.77	257.40	p < 0.001
threat susceptibility	2.62	0.76	2.28	0.75	2.49	0.93	2.06	0.68	24.79	p < 0.001
self-efficacy	4.33	0.72	4.67	0.53	4.36	0.91	2.94	0.99	133.41	p < 0.001
response efficacy	4.23	0.61	4.56	0.56	4.55	0.71	3.81	0.85	24.97	p < 0.001
formal sanction severity	2.77	0.94	2.56	0.91	2.73	0.89	2.27	0.69	133.98	p < 0.001
informal sanction severity	3.24	0.96	3.33	0.94	3.26	0.81	2.17	0.87	4.62	p < 0.05
formal sanction certainty	2.47	0.82	2.53	0.95	2.66	1.05	2.37	0.82	28.66	p < 0.001
informal sanction certainty	2.69	0.97	2.83	0.85	2.75	0.89	2.28	0.71	36.07	p < 0.001
sanction celerity	2.65	0.73	2.61	0.79	2.81	0.78	2.44	0.75	133.49	p < 0.001
compliance intention	3.21	0.75	3.29	0.72	3.29	0.80	2.24	0.96	9.90	p < 0.05

Descriptive Information and Test of Internal Validity

The respondents to the study were roughly even in terms of women and men and ranged in age from 18 to over 60. The most common age range was 50 to 59 (32.9%), and the most commonly reported education level was the bachelor's degree (27.3%). The full set of sample demographics is reported in Table 2.

The primary data revealed that the mean distributions across both the conventional and enhanced fear appeal rhetorical elements are fairly consistent across the three fear appeal types, but differ significantly in the control group to which no fear appeal was provided (see Table 3). The results of the MANOVA F-test comparison of mean values between these two groups supported this claim. Given that each of these elements is addressed within the language of the fear appeal, the significant differences in perceptions following exposure to the appeal are not surprising, which provides some assurance of the internal validity of the experimental design.

Results

We used SmartPLS to conduct a partial least squares (PLS) analysis of the research model for the survey data obtained following each type of fear appeal message. This approach to structural equation modeling (SEM) has advantages over a covariance-based SEM technique, such as LISREL, when the model in question is used for predictive purposes instead of theory testing purposes (Chin et al. 2003; Gefen and Straub 2005; Siponen and Vance 2010). In this analysis, our first step was to follow a PLS approach to validate the measurement model, as put forth by Gefen and Straub (2005). The process and outcomes of the measurement model validation tests are documented in Appendix B and include the results of tests for convergent and discriminant validity. The results of these tests indicated that our model demonstrates an acceptable level of measurement validity (Gefen and Straub 2005).

Model Testing

Similar to Siponen and Vance (2010), we took a multistage approach to analyzing the research model. Following this approach, we first examined the influence of control variables on compliance intention and then added (1) the conventional fear appeal and (2) sanction rhetorical elements, respectively, in subsequent stages of model testing.

Included in the control variables were gender, age, work experience, education, and fear appeal message type. Gender, age, work experience, and education were included to determine whether any of these variables had an effect on compliance intention. Fear appeal message type was included because there was interest in determining whether the fear appeal message and the threat/behavior pairs that articulated the messages were distinctive in their effect on compliance intentions. These control variables were able to explain 15 percent of the variance of intention, but only age ($\beta = 0.142$; $p < 0.05$) had a significant effect in this stage of the model testing. These results are presented in the First Stage Model results in Table 4.

In the next stage of the analysis, we added the conventional fear appeal rhetorical elements of threat severity, threat susceptibility, self-efficacy, and response efficacy to the previous model. The analysis of the additive effects of these elements on compliance intention revealed that three elements were significant determinants of compliance intention: response efficacy was the most influential factor ($\beta = 0.263$; $p < 0.05$), followed by threat severity ($\beta = 0.194$; $p < 0.05$), and self-efficacy ($\beta = 0.112$; $p < 0.05$). Age was no longer a significant determinant of compliance intention. Collectively, the elements were able to explain 26 percent of the variance in compliance intention. It should also be noted that threat severity formed significant relationships with both response efficacy ($\beta = 0.409$; $p < 0.05$) and self-efficacy ($\beta = 0.448$; $p < 0.05$), but threat susceptibility was nonsignificant in similar relationships. The results of this stage of testing are presented in the Second Stage Model results in Table 4.

To determine whether the inclusion of the conventional fear appeal rhetorical elements in the model resulted in a significant increase in explained variance in compliance intention, we used the following formula to assess first the effect size: $f^2 = (R^2 \text{ Full Model} - R^2 \text{ Partial Model})/(1\text{-}R^2 \text{ Full Model})$ (Chin et al. 2003). The effect size was calculated at 0.15. Based on this result, a pseudo F-test was calculated by taking the product of the effect size (f^2) and $(n - k - 1)$, where n is the sample size and k is the number of independent variables (Mathieson et al. 2001; Siponen 2000). The results of this F-test ($F = 65.70$, $p < .001$) suggested that, collectively, the conventional fear appeal rhetorical elements explained significantly more variance in compliance intention than the control variables alone did. The results of this multistage analysis are also summarized in Table 4.

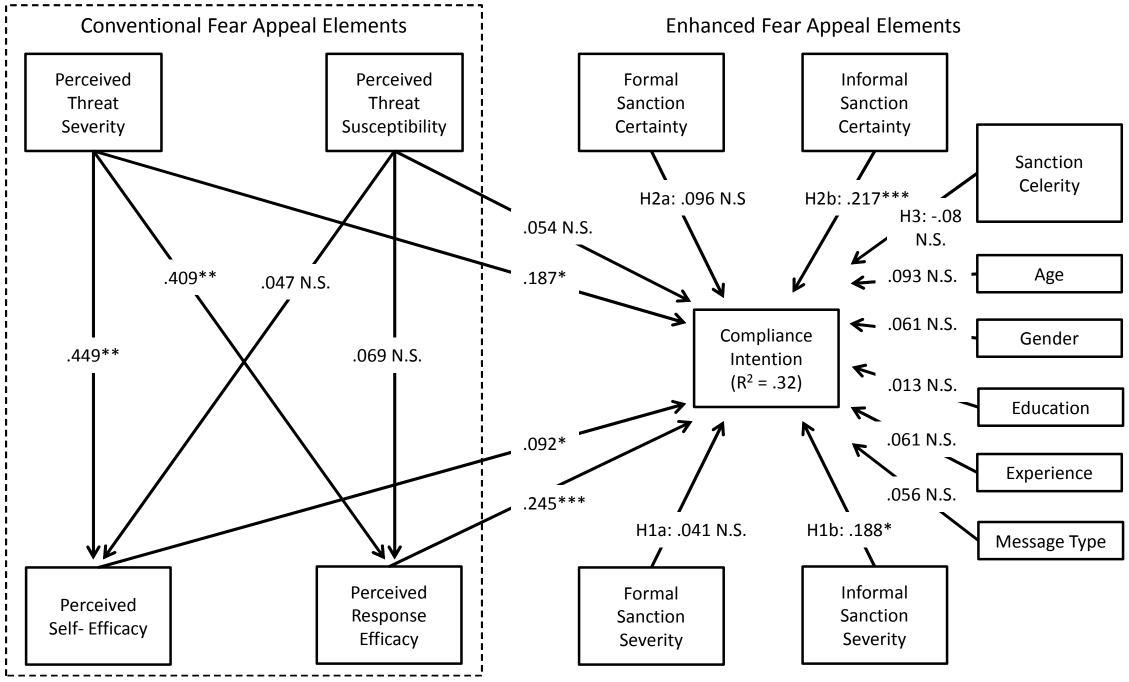
In the third and final stage of the multistage analysis, we included the deterrence rhetorical elements, accounting for both formal and informal varieties of sanction severity and sanction certainty. Sanction celerity was also included in this final stage of the analysis. As illustrated in Figure 3 and displayed in the Third Stage Model results in Table 4, the total explained variance increased to 32 percent, with informal sanction severity ($\beta = 0.188$; $p < 0.05$) and informal sanction certainty ($\beta = 0.217$; $p < 0.05$) serving as significant determinants of compliance intention. The effect size was calculated at 0.08. We also determined whether the inclusion of sanctioning rhetoric in the model resulted in a significant increase in explained variance in compliance intention. The results of this F-test ($F = 34.64$ $p < .001$) suggest that, collectively, perceived sanctions explained significantly more variance in compliance intention than the conventional fear appeal rhetoric alone did.

These findings support hypotheses H1b and H2b. The influence of sanction celerity on compliance intention was nonsignificant, thereby supporting H3. Because H3 is a null hypothesis, a *post hoc* power analysis using G*Power v3.1.3 was conducted and revealed the achieved power to be 0.99,

Table 4. Structural Model Results

	First Stage Model (control variables)	Second Stage Model (control variables + conventional fear appeal)	Third Stage Model (control variables + conventional fear appeal + sanctions)
R²	0.15	0.26	0.32
ΔR²	–	0.11	0.06*
Effect size	–	0.15 (medium)	0.08 (small)
Gender	0.157	0.070	0.061
Age	0.142**	0.078	0.093
Work Experience	0.004	0.018	0.061
Education	0.026	0.020	0.013
Fear Appeal Message Type	0.043	0.043	0.056
Threat Severity		0.194**	0.187*
Threat Susceptibility		0.006	0.054
Self-Efficacy		0.112*	0.092*
Response Efficacy		0.263***	0.245***
Formal Sanction Severity			0.041
Informal Sanction Severity			0.188*
Formal Sanction Certainty			0.096
Informal Sanction Certainty			0.217***
Sanction Celerity			-0.080

Notes: Standardized coefficients reported.
*p < .05; **p < .01; ***p < .001.



N.S. = Not Supported; *p < 0.05; **p < .01; ***p < .001

Figure 3. Summary of Results

which represents extremely high statistical power for detecting the small observed effect size. Similarly, the influence of formal sanction certainty and severity on compliance intentions was nonsignificant. These findings are nonsupportive of hypotheses H1a and H2a. The effects of the conventional fear appeal rhetorical elements of threat severity, self-efficacy, and response efficacy on compliance intention all remained significant, while threat susceptibility remained nonsignificant.

Finally, we used a PLS-pooled significance test for the multigroup analysis approach to detect significant differences in path coefficients for relationships involving the conventional fear appeals in the second- and third-stage models. In doing so, we were able to assess accurately the nature of the impact of the conventional fear appeal rhetorical elements on compliance intention when the sanctions were accounted for in the third stage model. In conducting the tests, t-statistics were used to assess the differences in path coefficients involving the conventional fear appeals across the second and third stage models, using the procedure first articulated by Chin, Marcolin, and Newsted (1996) and later successfully applied by Keil et al. (2000) and Ahuja and Thatcher (2005). The results of the t-test multigroup analysis indicated no significant difference in the path coefficients, suggesting that while the coefficient values of three of the four conventional fear appeal elements were technically of lesser value, when we accounted for sanctioning, the difference was nonsignificant.

Discussion

The review of the empirical results described above revealed several key findings, each of which contributes to both theory and practice. First, sanctioning rhetoric is able to enhance the effectiveness of a fear appeal, thus leading to stronger intentions to comply with information security policy. This finding confirms our contention that threats to the human asset complement those to the information asset in forming a more robust rhetorical composition of fear appeal. It is also interesting in that it explained the observance of compliance behavior among insiders, even when they lacked the necessary perception of impending threat, instead seeking to alleviate the possibility of embarrassment among peers. While our findings did not allow us to indicate the precise point at which a fear appeal can elicit diminished perceptions of threat or efficacy and still remain effective through the addition of sanctioning rhetoric, they did support this possibility and highlighted the beneficial effects of the human asset threat in general and sanctioning rhetoric in particular on the effectiveness of fear appeal.

A second important finding pertains to the findings from the three threat/response pairs, in which the conventional fear appeal rhetorical elements were tested. The findings of this study are generally consistent with earlier works involving the application of PMT to model the influence of conventional fear appeal rhetoric as a means of end user behavioral modification (Herath and Rao 2009; Johnston and Warkentin 2010). Other works involving PMT have posited competing outcomes, with little progress in the repeatability of findings (Bélanger and Crossler 2011). Tests of the research model using three distinct threat/response pairs embedded within three separate fear appeal messages revealed consistent correlations among the conventional fear appeal elements and compliance intention, and threat susceptibility was not a significant determinant in intentions to comply with recommended protective strategies. We again highlight this outcome as evidence of the inadequacy of the conventional fear appeal rhetorical composition and the subsequent misspecification of PMT within the information security context. Conventional fear appeal design and PMT do not distinguish between threats to the human asset and threats to information assets. Fear appeals modeled without this awareness will result in similar outcomes.

A third important finding involves the testing of distinct measures of sanctions, including sanction celerity and both formal and informal dimensions of sanction severity and sanction certainty. In our study, sanction celerity and the formal dimensions of sanction severity and sanction certainty were determined to be nonsignificant in their predictive influence on compliance intention, while informal sanction severity and informal sanction certainty were found to be significant in their roles as direct determinants of compliance intention. These results suggest that the prospect of losing the regard of colleagues (informal sanctions) is a significant motivation to engage in recommended protective strategies, perhaps because of the less discrete nature of informal sanctions, compared to formal sanctions. Previous studies also support informal sanctions as significant deterrents of intention to violate information security policy, and formal sanctions were found insignificant in this role (albeit in the absence of neutralization) (Siponen and Vance 2010).

Implications for Research

This study's primary implication for further research is the exposure of problems in previous applications of the conventional fear appeal rhetorical composition and the fear appeal behavioral modeling theory, PMT, in the information security context. To resolve these problems, we developed and tested an enhanced fear appeal rhetorical framework. Based on our results, we make the following contributions.

First, we demonstrate the inadequacy of the contemporary fear appeal *mechanism* as originally designed by Rogers (1975) when it is applied to the context of information security threats, and we offer a solution to this problem of inadequacy in the form of sanctioning rhetoric. Our focus is on the redesigning and testing of a long-standing artifact: the fear appeal mechanism. No study has demonstrated that the rhetorical components of a fear appeal are context dependent, nor has any study attempted to reconstitute an effective rhetorical composition for fear appeal messages regarding threats to information security. Given the prevalence of fear appeals in security management communication strategies and their inclusion in information security research studies, we believe this finding is an important contribution to the research.

Second, we demonstrate that fear appeals should highlight sanctioning rhetoric instead of traditional threat and efficacy rhetoric because when combined within the same message, sanctioning rhetoric is more influential. It may be argued that the integration of PMT and sanctions has already been accomplished (Herath and Rao 2009) and that the findings of this study are similar to those of purely sanction-based studies of security compliance. However, we argue that while Herath and Rao (2009) developed and tested an integrated model of PMT and general deterrence, the current study focusses on the behavioral change mechanism (i.e., the fear appeal) instead of the theory used to model the resultant behavior. Neither Herath and Rao nor any previous study has examined the limitations of the fear appeal mechanism for which PMT was developed to understand its impact. We reiterate that the present contribution is focused on the *mechanism* of behavior change, not the behavioral model used to predict its impact. This is new knowledge and explains why people may enact recommended behaviors even when they do not view a particular threat as menacing or personally relevant.

It could also be argued that if sanctions provide personal relevance, why include the PMT-based aspects of fear appeals? We point out that, regardless of the personal relevance attached to threats to data, information, and so on, these threats do exist, are real, and employees must be warned about them and provided with recommendations for protection against them. Therefore, the conventional fear appeal rhetoric describing these threats and threat response recommendations are necessary workplace requirements and have been and will continue to be used.

Third, from a behavioral modeling perspective, we also point out that PMT has been misspecified in the information security literature and the reason that misspecification has occurred. We also provide a means by which to overcome its misspecification without simply avoiding the use of fear appeals to warn against threats to non-personally relevant threats. This represents new knowledge and is a key component of our overall contribution. We also provide a direct answer to questions posed by scholars regarding why PMT-based findings within the information security literature are inconsistent with theoretical expectations and are therefore incongruent. We also generalize these arguments to reinforce the claims of Truex et al. (2006) and of Weber (2012) that all referent discipline theories need to be scrutinized carefully when they are applied in the study of a new phenomenon.

PMT was designed to explain how individuals react to fear-inducing stimuli. The fear appeals that were studied were primarily concerned with health or safety-related threats. These threats were to the physical self and were universally personally relevant. The fear appeals designed according to these types of threats have had relatively consistent success. However, because fear appeals and fear appeal theory (i.e., PMT) were adopted by information security scholars for use within the information security context, an underlying assumption was overlooked by both scholars and practitioners; thus, scholarship in this area has suffered. The overlooked underlying assumption was that the threats espoused in fear appeals *must* have personal relevance to the recipient. The dominant logic behind the application of fear appeals and PMT to information security phenomena was that threats to data, information, systems, and so on would be regarded in the same manner as threats to one's personal safety or health and have universal, personal relevance. We challenge this flawed logic. PMT does not account for the distinction in the nature of the espoused threat and, therefore, has been repeatedly misspecified in the security literature.

This study's contribution to research, as discussed above, was explicitly described by Locke and Golden-Biddle (1997) as problematizing the extant literature as incommensurate. Incommensurability emphases the invalidation of the applications of previous theory to a particular phenomenon, indicating that the candidate theory cannot sufficiently address the focal phenomenon and in fact would lead to poor conclusions or understanding. By pointing out the problem of incommensurability in the extant information security literature in its application of PMT, we have contributed to the theory in a meaningful manner (Locke and Golden-Biddle 1997). A significant theoretical contribution can be made by identifying a problem in the way in which a theory has been described or used. We make this claim in our discussion of PMT misspecification within the information security literature and offer a resolution to the problem.

Our study also contributes to the theory in terms of identifying intertextual noncoherence. Locke and Golden-Biddle defined intertextual noncoherence as the explicit presence of discord among scholars in terms of how the extant research describes agreement among scholars regarding a particular area of research. The current literature on the motivation for protective security actions provides explicit evidence of contradictory findings among scholars. For instance, Crossler (2010, p. 8) stated that his findings were "contrary to findings in the social psychology literature" and suggested that further research is needed to add congruence among scholars regarding the explanation of protective security behaviors. Anderson and Agarwal (2010, p. 637) suggested that research involving PMT should be extended to consider the specificity of the target of protection, suggesting a lack of consensus among scholars over what constitutes "a sense of ownership toward different objects and because the factors influencing behavior vary depending on the target." After finding unexpected results from the application of PMT to IT threat avoidance, Liang and Xue (2010, p. 404) contended that "further research on refined cognitive processes under threat is needed to find out which explanation [theirs or extant research expectation] is closer to the truth." Infinedo (2012) found that his application of PMT diverged from the expectations established in the literature and suggested the existence of a conceptualization problem among scholars in modeling threat appraisal. Finally, Vance et al. (2012, p. 194) contended that their threat vulnerability findings were "not consistent with PMT, [but are] consistent with other findings in the IS security domain." Consistent with Locke and Golden-Biddle's description of contributions through incommensurability problematization and intertextual noncoherence, we present an alternative rhetorical framework, which we argue is preferable to existing fear appeal and PMT applications to information security phenomena.

Finally, the present study also establishes a new baseline for the role of formal and informal sanctions. There are continued debates and inconsistent findings pertaining to the potential influence of informal and formal sanctions on compliance outcomes. Some studies have supported their influence (Kankanhalli et al. 2003; Siponen et al. 2007) and others have offered conflicting results (Siponen and Vance 2010). Our exhaustive literature search yielded no studies that have approached this question from the level of granularity as the present study, separately testing the formal and informal elements of sanction severity and certainty. Hence, our findings contribute to the debate and hopefully aid in the pursuit of consistency in information security violation deterrence research. Future research is needed, however, to continue this stream and add stability to the study of this phenomenon.

For instance, given the evidence for the strong influence of informal sanctions on policy compliance intentions presented in this study, future research should examine the role of social structures, including social networks and informal social learning environments, in supporting policy initiatives within organizational settings. This may be conducted by looking to the various insider communities that make up an organization and the role of the collective in persuading individual compliance activities. Informal social learning environments include the social networks that permeate an organization and offer unstructured reinforcement of protective behaviors through shared stories and vicarious experiences. The stronger these environments are, the more substantial the impact of informal sanctioning. The informal social learning environment is facilitated by the verbal support from peers and administrators, by the observations of others (vicarious experience), and by the situational support of protective behaviors provided by the organization (Warkentin et al. 2011). Hence, "water cooler" talk is important in fostering secure behaviors among employees, which the findings of this research support. Informal sanctions emerge from these interactions. Future research in this area would further our understanding of sanctioning as a compliance motivation tool, while simultaneously addressing the community-level perspective missing from the information security literature (Vroom and von Solms 2004).

Further research is also needed to isolate and understand the manner in which enhanced fear-based persuasive messages are interpreted, processed, and reinforced over time, in addition to incorporating influential effects, such as priming, message persistence, and fit with personality type and other dispositional factors. To address these potentially powerful influences, future research should follow subjects longitudinally to assess their perceptions as they evolve. Using this expanded set of empirically supported campaign elements, managers could identify and select an appropriate mix of statements that would provide the best overall strategy in influencing their employees to comply with recommended security policies and procedures.

Implications for Practice

The implications of this study suggest a departure from communication strategies involving conventional fear appeals. Our results suggest that persuasive message campaigns should focus on informal sanctions, such as reminding insiders to avoid "letting down your colleagues" or "losing the respect of your peers." This aspect of persuasive messaging is often undervalued in favor of formal sanctions that are devised and espoused by administratively controlled events or propaganda and tied directly to the severity and context of the violation in question. As is often the case, social forces are likely to shape the manner in which informal sanctions are communicated and delivered. Managers can leverage our findings within their specific organizational culture to identify the most effective manner in which to deliver effective campaigns that may combine elements of appeals to traditional protection motivation factors as well as appeals to sanction (pain) avoidance, especially informal sanctions. For managers, this means that SETA and other communications should encourage the development of an environment that includes informal gatherings that could facilitate the use of informal sanctions.

The outcomes of this research should be particularly interesting to security managers seeking to motivate insiders to comply with protective security actions that are typically associated with less harmful dangers, or those less well-known or understood by the general population of insiders, such as cases in which the traditional fear appeal formulation is not likely to have had the desired effect. Furthermore, in organizations in which certain protective security behaviors are mandated, our findings indicate the benefit of incorporating sanctioning rhetoric into fear-based persuasive messages that are meant to "scare" insiders into following prescriptive orders. The enhanced fear appeal is more effective than the conventional variety.

Limitations

As in many behavioral security research studies, a key limitation of the current research is the use of intention as opposed to actual behavior as the dependent variable. The question of progression from intention to actual behavior gives pause to many, but it can be supported by numerous works in criminology where intention is viewed as indicative of a precondition to a behavioral act (Paternoster and Simpson 1996). Furthermore, previous studies have also demonstrated a clear linkage between intention and actual behavior (Fishbein and Ajzen 1975). In the IS literature, numerous studies have positioned intention as the dependent variable, including van der Heijden (2004), Anderson and Agarwal (2010), and Siponen and Vance (2010), among many others. Therefore, although we do recognize that the absence of a measure of actual compliance behavior is a limitation of this study, we contend that the compliance intention measure is a serviceable approximation of behavior, thereby providing valuable insight into information security policy compliance outcomes.

Another limitation of this study concerns the sample, which was comprised of the insiders of a large city government in Finland. Concerns regarding this sample are centered on the governmental nature of the organization from which it was derived as well as the potential for cultural effects (Leidner and Kayworth 2006), both of which may lead to limitations in the generalizability of the findings (Lee and Baskerville 2003). Care must be taken when attempting to apply the findings of this study to traditional business environments, which are perhaps characterized by fewer regulations or financial limitations. Caution should also be taken in generalizing these results to other cultures because cultural norms and dynamics may uniquely influence individual perceptions and relationships with the organization (Schneider 1989), particularly in the area of behavioral information security (Dinev et al. 2006; Wasti 2003).

Another limitation of the study concerns the potential for response bias. In any research study in which subjects are asked to report their intentions to violate social norms or policies, there is the potential for response bias, acquiescence bias, or social desirability bias. However, in this study, our subjects were guaranteed anonymity, which minimized this concern. Furthermore, the subjects were informed by the study administrators that their participation in the study and submission of truthful responses would yield no negative consequences.

Conclusion

Fear appeals have been widely applied in the study of information security phenomena, but previous research has achieved mixed results and only marginal success. We argue that the reason for these disappointing results stems from the inadequacy of the conventional fear appeal rhetorical framework and the misspecification of PMT within the information security literature, in which scholars have consistently overlooked the underlying assumption that the espoused threats must have personal relevance for the fear appeal audience. The conventional fear appeal rhetoric and PMT do not account for the distinction between threats to one's self and threats to one's data property. This study develops and tests an enhanced fear appeal rhetorical framework that accounts for the distinction between threats to information assets and threats to human assets. By leveraging a purposeful juxtaposition of PMT and deterrence theory, we embed sanctioning rhetoric in conventional rhetoric to achieve greater levels of employee intention to comply with information security policies that involve the adoption of protective behaviors. Although some employees may be more motivated by protection and others may be influenced more by the desire to avoid personal pain through informal sanctions, the cumulative effect on the workforce of combining both elements should be positive.

Acknowledgments

We thank the anonymous reviewer who provided the discerning perspective on our theoretical contributions and the role of our work in the context of the extant published literature on PMT and deterrence. We have incorporated his questions into our discussion. We also thank Senior Editor Viswanath Venkatesh, whose diligent guidance and attention to detail was an invaluable asset in the process and was instrumental to our success. This research was funded by the Academy of Finland and the Finnish Funding Agency for Technology and Innovation (TEKES).

References

AHIMA. 2011. "Sanction Guidelines for Privacy and Security Violations," *Journal of AHIMA* (82:10), pp. 66-71.

Ahuja, M. K., and Thatcher, J. B. 2005. "Moving Beyond Intentions and Toward the Theory of Trying: Effects of Work Environment and Gender on Post-Adoption Information Technology Use," *MIS Quarterly* (29:3), pp. 427-459.

Akers, R. 1990. "Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken," *The Journal of Criminal Law and Criminology* (81:3), pp. 653-676.

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp. 613-643.

Angst, C. M., and 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), pp. 339-370.

ASPECT Consortium. 2004. "Tobacco or Health in the European Union: Past, Present and Future," Luxembourg: Office ofor Official Publications of the European Communities (http://ec.europa.eu/health/archive/ph_determinants/life_style/tobacco/documents/tobacco_fr_en.pdf).

Avgerou, C. 2013. "Social Mechanisms for Causal Explanation in Social Theory Based IS Research," *Journal of the Association for Information Systems* (14:8), pp. 399-419.

Bartholomew, L. K., Parcel, G. S., Kok, G., Gottlieb, N. H., and Fernandez, M. E. 2011. *Planning Health Promotion Programs: An Intervention Mapping Approach* (3rd ed.), San Francisco: Jossey-Bass.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017-1042.

Burnkrant, R. E., and Unnava, H. R. 1989. "Self-Referencing: A Strategy for Increasing Processing of Message Content," *Personality and Social Psychology Bulletin* (15:4), pp. 628-638.

Center for Substance Abuse Prevention. 2012. "Social Marketing and Health Communications," Substance Abuse and Mental Health Services Administration, CSAP Training Library.

Chin, W., Marcolin, B., and Newsted, p. 2003. "A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic Mail Emotion/Adoption Study," *Information Systems Research* (14:2), pp. 189-217.

Comello, M. L. G., and Slater, M. D. 2011. "The Effects of Drug-Prevention Messages on the Accessibility of Related Constructs," *Journal of Health Communication* (16:5), pp. 458-469.

Crossler, R. E. 2010. "Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data," in *Proceedings of the 43rd Hawaii International Conference on System Sciences*, Los Alamitos, CA: IEEE Computer Society Press, pp. 1-10.

D'Arcy, J., and Devaraj, S. 2012. "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model," *Decision Sciences* (43:6), pp. 1091-1124.

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643-658.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

de Hoog, N., Stoebe, W., and de Wit, J. B. F. 2005. "The Impact of Fear Appeals on Processing and Acceptance of Action Recommendations," *Personality and Social Psychology Bulletin* (31:1), pp. 24-33.

de Hoog, N., Stroebe, W., and de Wit, J. B. F. 2007. "The Impact of Vulnerability to and Severity of a Health Risk on Processing and Acceptance of Fear-arousing Communications: A Meta-Analysis," *Review of General Psychology* (11:3), pp. 258-285.

Dinev, T., Bellotto, M., Hart, P., Russo, V., and Serra, I. 2006. "Privacy Calculus Model in e-Commerce: A Study of Italy and the United States," *European Journal of Information Systems* (15:4), pp. 389-402.

Dutta, M. J., and Vanacker, B. 2000. "Effects of Personality on Persuasive Appeals in Health Communication," *Advances in Consumer Research* (27:1), pp. 119-124.

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention and Behavior,* Reading, MA: Addison-Wesley.

Gefen, D., and Straub, D. 2005. "A Practical Guide to Factorial Validity Using PLS-graph: Tutorial and Annotated Example," *Communications of the AIS* (16:5), pp. 91-109.

Gibbs, J. P. 1975. *Crime, Punishment, and Deterrence,* New York: Elsevier North-Holland.

Grover, V., Lyytinen, K., Srinivasan, A., and Tan, B. C. Y. 2008. "Contributing to Rigorous and Forward Thinking Explanatory Theory," *Journal of the Association for Information Systems* (9:2), pp. 40-47.

Harrington, S. J. 1996. "The Eeffect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgements and Intentions," *MIS Quarterly* (20:3), pp. 257-278.

Hastings, G., Stead, M., and Webb, J. 2004. "Fear Appeals in Social Marketing: Strategic and Ethical Reasons for Concern," *Psychology and Marketing* (21:11), pp. 961-986.

Herath, T., and Rao, H. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Hollinger, R. C., and Clark, J. P. 1982. "Formal and Informal Social Controls of Employee Deviance," *The Sociological Quarterly* (23:3), pp. 333-343.

Hornik, R., Jacobson, L., Orwin, R., Piesse, A., and Kalton, G. 2008. "Effects of the National Youth Anti-Drug Media Campaign on Youths," *American Journal of Public Health* (98), pp. 2229-2236.

Hovland, C., Janis, I. L., and Kelly, H. 1953. *Communication and Persuasion,* New Haven, CT: Yale University Press.

Howe, E. S., and Loftus, T. C. 1996. "Integration of Certainty, Severity, and Celerity Information in Judged Deterrence Value: Further Evidence and Methodological Equivalence," *Journal of Applied Social Psychology* (26:3), pp. 226-242.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?," *Communications of the ACM* (54:6), pp. 54-60.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1), pp. 83-95.

Janis, I. L. 1967. "Effects of Fear Arousal on Attitude Change: Recent Developments in Theory and Experimental Research," in *Advances in Experimental Social Psychology,* L. Berkowitz (ed.), New York: Academic Press, pp. 166-225.

Janis, I. L., and Feshbach, S. 1953. "Effects of Fear-Arousing Communications," *Journal of Abnormal and Social Psychology* (48:1), pp. 78-92.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Kankanhalli, A., Teo, H.-H., Tan, B., and Wei, K.-K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2), pp. 139-154.

Kaplan, B., and Duchon, D. 1988. "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study," *MIS Quarterly* (12:4), pp. 571-586.

Keller, P. A., and Block, L. G. 1996. "Increasing the Persuasiveness of Fear Appeals: The Effect of Arousal and Elaboration," *Journal of Consumer Research* (22:4), pp. 448-460.

Keil, M., Tan, B. C. Y., Wei, K. K., Saarinen, T., Tuunainen, V., and Wassenaar, A. 2000. "A Cross-Cultural Study on Escalation of Commitment Behavior in Software Projects," *MIS Quarterly* (24:2), pp. 299-325.

Lee, A. S., and Baskerville, R. L. 2003. "Generalizing Generalizability in Information Systems Research," *Information Systems Research* (14:3), pp. 221-243.

Lee, Y. 2011. "Understanding Anti-Plagiarism Software Adoption: An Extended Protection Motivation Theory Perspective," *Decision Support Systems* (50:2), pp. 361–369.

Lee, Y., and Larsen, K. R. 2009. "Threat or Coping Appraisal: Determinants of SMB Executive's Decision to Adopt Anti-Malware Software," *European Journal of Information Systems* (18:2), pp. 177-187.

Leidner, D., and Kayworth, T. 2006. "*Review*: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict," *MIS Quarterly* (30:2), pp. 357-399.

Leventhal, H. 1970. "Findings and Theory in the Study of Fear Communications," in *Advances in Experimental Social Psychology 5,* L. Berkowitz (ed.), New York: Academic Press, pp. 119-186.

Leventhal, H. 1971. "Fear Appeals and Persuasion: The Differentiation of a Motivational Construct," *American Journal of Public Health* (61:6), pp. 1208-1224.

Li, H., Sarathy, R., Zhang, J., and Luo, X. 2014. "Exploring the Effects of Organizational Justice, Personal Ethics and Sanction on Internet Use Policy Compliance," *Information Systems Journal* (24:6), pp. 479-502.

Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1), pp. 71-90.

Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11:7), pp. 394-413.

Locke, K., and Golden-Biddle, K. 1997. "Constructing Opportunities for Contribution: Structuring Intertextual Coherence and 'Problematizing' in Organizational Studies," *Academy of Management Journal* (40:5), pp. 1023-1062.

MacKenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011. "Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques," *MIS Quarterly* (35:2), pp. 293-334..

Maddux, J. E., and Rogers, R. W. 1983. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* (19:5), pp. 469-479.

Mathieson, K., Peacock, E., and Chin, W. 2001. "Extending the Technology Acceptance Model: The Influence of Perceived User Resources," *The DATABASE for Advances in Information Systems* (32:3), pp. 86-112.

McGuire, W. J. 1968. "Personality and Susceptibility to Social Influence," in *Handbook of Personality Theory and Research,* E. Borgatta and W. Lambert (eds.), Chicago: Rand McNally, pp. 1130-1187.

Milne, S., Sheeran, P., and Orbell, S. 2006. "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory," *Journal of Applied Social Psychology* (30:1), pp. 106-143.

Morales, A. C., Wu, E. C., and Thomas, R. D. 2012. "How Disgust Enhances the Effectiveness of Fear Appeals," *Journal of Marketing Research* (49:3), pp. 383-393.

Ng, B. Y., Kankanhalli, A., and Xu, Y. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (46:4), pp. 815-825.

O'Keefe, D. J. 1990. *Persuasion: Theory and Research,* Newbury Park, CA: Sage Publications.

Oswick, C., Fleming, P., and Hanlon, G. 2011. "From Borrowing to Blending: Rethinking the Process of Organizational Theory Building," *Academy of Management Review* (36:2), pp. 318-337.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards IS Security Policy Compliance," in *Proceedings of the 40th Hawaii International Conference on System Sciences*, Los Alamtios, CA: IEEE Computer Society Press, p. 156b.

Paternoster, R., and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law & Society Review* (30:3), pp. 549-583.

Peters, G. Y., Ruider, R. A. C., and Kok, G. 2013. "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), pp. 71-79.

Petty, R. E., and Cacioppo, J. T. 1986. "The Elaboration Likelihood Model of Persuasion," *Advances in Experimental Social Psychology* (19), pp. 123-205.

Piquero, A. R., and Tibbetts, S. G. 1996. "Specifying the Direct and Indirect Effects on Low Self-Control and Situational Factors in Offenders Decision Making: Toward a More Comparative Model of Rational Offending," *Justice Quarterly* (13:3), pp. 481-510.

Podsakaoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Rresearch: A Critical Review of the Literature and Recommended remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.

Ponemon Institute. 2012. "2011 Cost of Data Breach Study," Traverse City, MI: Research Department, Ponemon Institute (http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf).

Pratt, T. C., and Cullen, F. T. 2000. "The Empirical Status of Gottfredson and Hirschi's General Theory of Crime: A Meta-Analysis," *Criminology* (38:3), pp. 931-964.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757-778.

Richardson, R. 2008. "CSI Computer Crime & Security Survey" (http://i.zdnet.com/blogs/csisurvey2008.pdf)

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91:1), pp. 93-114.

Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protected Motivation," in *Social Psychophysiology: A Sourcebook*, J. T. Cacioppo and R. E. Petty (eds.), New York: The Guilford Press, pp. 153-176.

Sasse, M. A., Brostoff, S., and Weirich, D. 2001. "Transforming the 'Weakest Link'—A Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal* (19:3), pp. 122-131.

Schneider, S. C. 1989. "Strategy Formulation: The Impact of National Culture," *Organization Studies* (10:2), pp. 149-168.

Shaw, E., Ruby, K. G., and Post, J. M. 1998. "The Insider Threat to Information Systems: The Psychology of the Dangerous Insider," *Security Awareness Bulletin* (2:98), pp. 1-10.

Siponen, M. T. 2000. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management and Computer Security* (8:1), pp. 31-41.

Siponen, M., Pahnila, S., and Mahmood, A. 2007. "Employees' Adherence to Information Security Policies: An Empirical Study," in *IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments*, H. Venter, M. Eloff, L. Labuschagne, J. Elof, and R. von Solms (eds.), Boston, MA: Springer, pp. 133-144.

Siponen, M., and Vance, A. O. 2010. "Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Slater, M. D. 2006. "Specification and Misspecification of Theoretical Foundations and Logic Models for Health Communication Campaigns," *Health Communications* (20:2), pp. 149-157.

Straub, D. W. 1989. "Validating Instruments in MIS Research," *MIS Quarterly* (13:2), pp. 147-169.

Straub, D. W. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

Straub, D. W., Carlson, P. J., and Jones, E. H. 1993. "Deterring Cheating by Student Programmers: A Field Experiment in Computer Security," *Journal of Management Systems* (5:1), pp. 33-48.

Straub, D. W., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organizational: A Field Study," *MIS Quarterly* (14:1), pp. 45-62.

Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Tittle, C. R., and Rowe, A. R. 1974. "Certainty of Arrest and Crime Rates: A Further Test of the Deterrence Hypothesis," *Social Forces* (52:4), pp. 455-462.

Truex, D., Holmström, J., and Keil, M. 2006. "Theorizing in Information Systems Research: A Reflexive Analysis of the Adaptation of Theory in Information Systems Research," *Journal of the Association for Information Systems* (7:12), pp. 797-821.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3-4), pp. 190-198.

van der Heijden, H. 2004. "User Acceptance of Hedonic Information Systems," *MIS Quarterly* (28:4), pp. 695-704.

Velicer, W. F., and Prochaska, J. O. 2008. "Stage and Non-Stage Theories of Behavior and Behavior Change: A Comment on Schwarzer," *Applied Psychology* (57:1), pp. 75-83.

Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the Qualitative–Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS Quarterly* (37:1), pp. 21-54.

Vroom, C., and von Solms, R. 2004. "Towards Information Security Behavioural Compliance," *Computers & Security* (23:3), pp. 191-198.

Wall, D. S. 2011. "Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders," White Paper: Data Loss Prevention, Symantec, Mountain View, CA (http://download.channelpartner.de/files/578.pdf).

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention," *European Journal of Information Systems*, (20:3), pp. 267-284.

Wasti, S. A. 2003. "Organizational Commitment, Turnover, Intentions and the Influence of Cultural Values," *Journal of Occupational and Organizational Psychology* (76:3), pp. 303-321.

Weber, R. 2012. "Evaluating the Developing Theories in the Information Systems Discipline," *Journal of the Association for Information Systems* (13:1), pp. 1-30.

Weirich, D., and Sasse, M. A. 2001. "Pretty Good Persuasion: A First Step Towards Effective Password Security in the Real World," in *Proceedings of the Workshop on New Security Paradigms*, Cloudcraft, New Mexico, pp. 137-143.

Williams, K., and Hawkins, R. 1986. "Perceptual Research on General Deterrence: A Critical Review," *Law and Society Review* (20:4), pp. 545-572.

Witte, K. 1992. "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," *Communication Monographs* (59:4), pp. 329-349.

Witte, K. 1994a. "Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM)," *Communication Monographs* (61:2), pp. 113-134.

Witte, K. 1994b. "Generating Effective Risk Messages: How Scary Should Your Risk Communication Be?," *Communication Yearbook* (18), pp. 229-254.

Witte, K. 1998. "Fear as Motivator, Fear as Inhibitor: Using the Extended Parallel Process Model to Explain Fear Appeal Successes and Failures," in *Handbook of Communication and Emotion: Research, Theory, Applications, and Contexts,* P. A. Andersen and L. K. Guerrero (eds.), San Diego, CA: Academic Press, pp. 423-450.

Witte, K., Cameron, K., McKeon, J., and Berkowitz, J. 1996. "Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale," *Journal of Health Communication* (1), pp. 317-341.

Woon, I. M. Y., Tan, G. W., and Low, R. T. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," in *Proceedings of the 26th International Conference on Information Systems*, D. Avison, D. Galletta, and J. I. DeGross (eds.), Las Vegas, NV, pp. 367-380.

About the Authors

Allen C. Johnston is an associate professor and the director of IS programs in the School of Business at the University of Alabama at Birmingham. The primary focus of his research is in the areas of behavioral information security, privacy, data loss prevention, and collective security and his research can be found in such outlets as *MIS Quarterly*, *European Journal of Information Systems*, *Communications of the ACM*, *Journal of Global Information Management*, *Journal of Organizational and End User Computing*, *Information Technology and People*, and *The DATABASE for Advances in Information Systems*. He currently serves as an associate editor for *European Journal of Information Systems* and *Journal of Information Privacy and Security*, serves on the Editorial Review Board for *The DATABASE for Advances in Information Systems*, and is a founding member of the IFIP Working Group on Information Systems Security Research (WG8.11/11.13). Allen has also served as a visiting professor or invited speaker at several universities and companies in the United States and abroad.

Merrill Warkentin is a professor of MIS and the Drew Allen Endowed Fellow in the College of Business at Mississippi State University. His research, primarily on the impacts of organizational, contextual, situational, and dispositional influences on individual computer user behaviors in the context of information security and privacy, has appeared in *MIS Quarterly, Decision Sciences, European Journal of Information Systems, Decision Support Systems, Computers & Security, Information Systems Journal, Communications of the ACM, Communications of the AIS, Journal of Information Systems*, and others, and he is the author or editor of several books on technology. Merrill has authored or coauthored over 250 published manuscripts, including over 50 journal articles. He is the AIS Departmental Editor for IS Security & Privacy, the chair of the IFIP Working Group on Information Systems Security Research (WG8.11/11.13), the vice president for Publications of the Decision Sciences Institute, and an associate editor for *MIS Quarterly, European Journal of Information Systems*, and *Information & Management*. He is senior editor of *AIS Transactions on Replication Research* and an Eminent Area Editor (MIS) for *Decision Sciences*. Merrill served as a national Distinguished Lecturer for the Association for Computing Machinery. His work has been funded by National Science Foundation, National Security Agency, Department of Defense, Homeland Security, IBM, and others. He has chaired several national and international conferences, has been track chair for the International Conference on Information Systems, Americas Conference on Information Systems, European Conference on Information Systems, and Decision Sciences Institute, and will be the program cochair of the Americas Conference on Information Systems in 2016. Merrill has served as a visiting professor or invited speaker at numerous universities in North America, Europe, and Asia.

Mikko Siponen is a professor in the Department of Computer Science and Information Systems at the University of Jyväskylä. He holds a Ph.D. in philosophy from the University of Joensuu, Finland, and a Ph.D. in Information Systems from the University of Oulu, Finland. His research interests include IS security, IS development, computer ethics, and philosophical aspects of IS. Mikko has published 45 articles in journals such as *MIS Quarterly*, *Journal of the Association for Information Systems*, *Information & Management*, *European Journal of Information Systems*, *Information & Organization*, *Communications of the ACM*, *IEEE Computer*, *IEEE IT Professional*, and others. He has received over 5 million EUR of research funding from corporations and numerous funding bodies. He has been a track chair for the International Conference on Information Systems and the European Conference on Information Systems three times. His other editorial board experiences include positions with *Journal of the Association for Information Systems, European Journal of Information Systems*, *Information & Management*, and *Communications of the Association for Information Systems.*