Journal of Management Information Systems
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/mmis20

Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective

John D'Arcy [a], Tejaswini Herath [b] & Mindy K. Shoss [c]
[a] University of Delaware
[b] Brock University
[c] Saint Louis University
Published online: 07 Dec 2014.

Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective

JOHN D'ARCY, TEJASWINI HERATH, AND MINDY K. SHOSS

JOHN D'ARCY is an assistant professor of MIS at the University of Delaware. He received his Ph.D. in business administration, with a specialization in MIS, from Temple University. His research areas include information security, IT risk management, and computer ethics. Journals in which his work appears include *Information Systems Research, Journal of Management Information Systems, European Journal of Information Systems, Decision Sciences,* and *Decision Support Systems.*

TEJASWINI HERATH is an associate professor of information systems at Brock University. She received her Ph.D. in management science and systems from the State University of New York–Buffalo. Her research interests are mainly in information assurance. Journals in which her work appears include *Journal of Management Information Systems, European Journal of Information Systems,* and *Decision Support Systems.* Her research has been funded by the Social Sciences and Humanities Research Council of Canada (SSHRC).

MINDY K. SHOSS is an assistant professor of psychology at Saint Louis University. She received her Ph.D. in industrial/organizational psychology from the University of Houston. Her research interests include employee stress, coping, health, and productivity. Journals in which her work appears include *Journal of Applied Psychology, Journal of Organizational Behavior,* and *Journal of Occupational Health Psychology.*

ABSTRACT: We use coping theory to explore an underlying relationship between employee stress caused by burdensome, complex, and ambiguous information security requirements (termed "security-related stress" or SRS) and deliberate information security policy (ISP) violations. Results from a survey of 539 employee users suggest that SRS engenders an emotion-focused coping response in the form of moral disengagement from ISP violations, which in turn increases one's susceptibility to this behavior. Our multidimensional view of SRS—comprised of security-related overload, complexity, and uncertainty—offers a new perspective on the workplace environment factors that foster noncompliant user behavior and inspire cognitive rationalizations of such behavior. The study extends technostress research to the information systems security domain and provides a theoretical framework for the influence of SRS on user behavior. For practitioners, the results highlight the incidence of SRS in organizations and suggest potential mechanisms to counter the stressful effects of information security requirements.

Journal of Management Information Systems / Fall 2014, Vol. 31, No. 2, pp. 285–318.

ISSN 0742–1222 (print) / ISSN 1557–928X (online)
DOI: 10.2753/MIS0742-1222310210

KEY WORDS AND PHRASES: coping theory, ethical orientation, information security, moral disengagement theory, sanctions, security compliance, security policies, security policy violation, social cognitive theory, technostress, workplace stress.

ACADEMICS AND PRACTITIONERS ALIKE RECOGNIZE EMPLOYEES as a major threat to organizational information security efforts [14, 69]. To address this "insider" threat, organizations have devoted significant resources into behavioral security measures, such as policy development and education and training, in addition to continually updating their security technologies [54]. U.S. federal and state governments and certain industries have also introduced regulations and standards that mandate organizations' internal security measures [14]. Despite these initiatives, a class of employee security–related behaviors known as *volitional (but not malicious) information security policy (ISP) violations* [27, 71] (e.g., password sharing, failing to log off when leaving workstation) continue to plague organizations. At least some explanation for this predicament is that employees face a surfeit of rapidly expanding security requirements (i.e., policies, procedures, and technical controls), which they find to be constraining, inconvenient, and difficult to understand [51, 53, 69]. Evidence of this comes from a recent survey of over 2,800 employees [16] in which "too busy to think about policies" and "policies are inconvenient to follow" were reported as chief reasons for ISP violations. Some authors have suggested that security requirements can backfire and bring about security-diminishing behavior due to the demands (e.g., time, effort, frustration) they impose on employees [51, 60, 64]. Although there is preliminary evidence to support this notion [51], the information systems (IS) literature lacks a systematic, theory-driven investigation of the potential adverse effects of organizational information security requirements (hereafter security requirements) on user behavior. A goal of this paper is to address this gap.

Against this backdrop, we offer a new avenue for understanding employees' ISP violations—namely, workplace stress due to security requirements and its coping response. The topic of stress has a long history in the organizational and psychology literatures and empirical results have shown that negative work stressors[1] predict a variety of undesirable employee behaviors (e.g., [25, 57]). Within the IS literature, research indicates that employee stress–related to the use information technology (IT) (i.e., technostress) influences a number of IT and non-IT-related cognitions and behaviors [56, 67]. In the present study, we extend the technostress concept to the domain of IS security and explain three conditions—overload, complexity, and uncertainty—in which security requirements can create stress in employees. We theorize that this form of employee stress, termed *security-related stress (SRS),* is a contributor to ISP violations.

Using coping theory as a foundation [38], we develop and empirically test a model of ISP violation intention which predicts that employees engage in emotion-focused coping in response to SRS. We explicate this emotion-focused coping in the form of

cognitive rationalization processes drawn from moral disengagement theory [6]. In this manner of coping, employees respond to SRS by disengaging their internal self-sanctions related to ISP violations, which in turn increases their ISP violation intention. Consistent with the deterrence literature, we also posit that perceived sanctions influence both moral disengagement and ISP violation intention. We empirically test our model using data collected through a survey of 539 employee users from a diverse set of organizations. The results support our multidimensional view of SRS[2]—which consists of security-related overload, complexity, and uncertainty—as a set of workplace environment factors that foster noncompliant user behavior, while extending prior work on employee rationalizations of ISP violations and the role of sanctions in security compliance decisions.

The paper proceeds as follows. The next section reviews relevant IS security literature, while the third section lays out the SRS concept and the theoretical foundation of the research. This is followed by the research model and hypotheses, and then the methodology and data analysis. The final section discusses the study's findings, implications for research and practice, limitations, and future research.

Background Literature

THERE IS GROWING BODY OF ACADEMIC IS SECURITY LITERATURE (e.g., [36, 74]), with a major emphasis on behavioral security issues (e.g., [19, 20, 42, 63, 71]) and ISP compliance in particular (e.g., [13, 14, 27, 32, 55]). The behavioral security research links numerous factors, including organizational sanctions, individual dispositions, security-related attitudes and beliefs, and workplace context, to name a few, to employees' security compliance decisions. Recent publications summarize the empirical literature on ISP compliance and related security behaviors [3, 62, 70].

Although this literature provides a solid foundation for understanding employees' security compliance decisions, our knowledge of the phenomenon remains incomplete. Evidence of this can be seen in the percentage of unexplained variance in existing security compliance models, which generally hovers in the 50–70 percent range for the behavioral outcome variable. A recent commentary by Willison and Warkentin [71] advocates a greater emphasis on factors traditionally considered outside the realm of IS security to study employee security-related phenomena. We follow this lead and draw upon topics from the organizational and psychology literatures, namely, workplace stress and its coping response, as drivers of ISP violations. Our conceptualization of workplace stress is, however, IS specific in that we focus on stress due to security requirements as opposed to generic workplace stress. There is some empirical support for security requirements as stressors and more generally for their negative effects on users. For example, Puhakainen and Siponen [55] documented employees' stressful reactions to a policy that required the secure use of e-mail. Herath and Rao [29] reported a significant negative relationship between severity of punishment for a security policy violation and compliance intention. Posey et al. [51] found that factors consistent with a dynamically changing security environment foster internal computer abuse. Bulgurcu et al. [13] found that perceived work impediment

increases the perceived cost of complying with security policies and thus indirectly reduces compliance intention. There is also evidence that computer monitoring can lead to negative perceptions of the organization and undesirable user behaviors [1, 52]. Beyond this work, we know of no research that has explored the potential negative consequences of security requirements, particularly in the context of ISP violations. Furthermore, the IS literature lacks a comprehensive definition of what constitutes negative or stressful security demands and thereby has yet to distinguish the aspects of security requirements that can engender stress and noncompliance. We seek to address these issues by proposing a coping-based theoretical model that depicts an underlying relationship between SRS and ISP violation intention. As described next, we draw from the technostress literature and conceptualize SRS in terms of overload, uncertainty, and complexity dimensions, and we delineate an emotion-based coping response to SRS based on moral disengagement theory.

Security-Related Stress and Theoretical Framing

Security-Related Stress

RESEARCHERS HAVE USED THE TERM *TECHNOSTRESS* to describe end user stress caused by accelerating technology demands in the workplace [4, 67]. We similarly use the term *security-related stress* to describe the stressful demands specifically imposed by security requirements. SRS is a form of psychological stress, and thus is stress caused by internal or external security-related demands appraised as taxing one's cognitive resources or abilities [38].

Stress itself is a complex concept that has mainly been defined and operationalized in terms of stimulating conditions (i.e., events impinging on the person) that produce stress reactions [37, 38]. In this vein, the IS literature provides the technostress creators construct, which delineates five stress-creating aspects of organizational IT usage: overload, invasion, complexity, insecurity, and uncertainty [56, 67]. These conditions reflect employees' attempts and struggles to deal with constantly evolving workplace technologies and the cognitive and social requirements related to their use [56, 67]. The technostress creators construct provides a tenable basis for our conceptualization of SRS, which deals with the stress-creating aspects of security requirements. We draw upon this construct and consider the overload, complexity, and uncertainty dimensions as most relevant in the IS security context.[3]

SRS overload describes situations where security requirements increase workload for employees and, as a result, create added time pressure for them to complete job duties. For example, employees who do not have administrative access to their work computers may have to spend valuable time completing paperwork and waiting for an IT professional to install needed software or download needed materials. As a result, employees have to work harder and faster to compensate for the overload caused by this security requirement. Another example is a centrally scheduled security maintenance task, such as an automated virus scan or patch update, which disrupts an employee's intended work task. Here the employee incurs a time penalty because his

or her workstation is either completely blocked from completing the intended task or slowed down to the point of ineffectiveness, thereby preventing other (possibly critical) tasks from being completed on time. In line with these examples, academic and practitioner studies indicate that employees view many security requirements as laborious and unnecessary overhead that impedes their productivity [16, 26, 51, 64, 69]. These conditions are known causes of frustration and stress [25, 47, 57]. Employees have also lamented that many security requirements force them to adapt their work procedures (e.g., not sharing passwords with coworkers) [12, 64], which can be stress inducing.

SRS complexity describes situations where security requirements are viewed as complex and thereby force employees to expend time and effort in learning and understanding security. For instance, to the extent that security policies involve multiple contingencies or contain technical jargon, employees will have to devote greater time and effort toward understanding the appropriate policy and deciding how to act. Because doing so diminishes time and energy resources available for the job-related tasks for which employees are evaluated and rewarded, complex requirements are likely a source of stress. To give more concrete examples, in the aforementioned study of a secure e-mail policy, one employee stated that "the security manual contains too much jargon, which makes it difficult to understand" [55, p. 767], while another commented that "I find it difficult to decide when encryption is really required" [55, p. 766]. In a separate study, an employee revealed a reluctance to ask for help with security matters "because it's stuff that everyone else knows and I should" [64, p. 170]. As exemplified by these comments and additional research [12, 16, 26], employees may have difficulty understanding security requirements, find them intimidating, and lack the knowledge and skills to comply, all of which can lead to stress.

SRS uncertainty refers to contexts where the organization continually updates and changes its job-related security requirements. Whether internally driven or as a result of government or industry regulations, organizations have faced an influx of security requirements in recent years, many of which have made their way into the daily job functions of employees [16, 54]. For example, evolving data breach notification laws and other security-based regulations (e.g., Sarbanes–Oxley Act [SOX], Payment Card Industry Data Security Standard [PCI DSS], Health Insurance Portability and Accountability Act [HIPAA]) have imposed new encryption rules for transmitting data and authentication procedures for accessing corporate systems (e.g., virtual private networks, biometric systems) [14, 16, 36]. Many industries also require periodic security training sessions that expose employees to new security requirements [54]. Organizations are also constantly managing the risks created by new technologies, which necessitates changing security requirements. One example is social media. As organizations discover additional risks and the social media landscape changes, they need to adapt and create additional policies. A consequence of the dynamic organizational security environment is that employees are constantly adjusting to new requirements, with little chance to develop a base of experience or assimilate security into their work routines. This uncertainty can be unsettling for employees and cause stress.

Extant research provides a strong basis for our representation of SRS. In particular, the overload, complexity, and uncertainty dimensions are consistent with several formal properties of stressful conditions (e.g., ambiguity, uncertainty, time sensitivity, uncontrollability) identified in the psychological stress literature [37, 38] and with several recognized negative work stressors, such as work overload, task difficulty, environmental uncertainty, situational restraints, and administrative hassles [25, 39, 49]. The SRS dimensions also resemble stressful conditions brought on by technological change [45] and incorporate research that points to ever increasing and constantly evolving security requirements as stress creators [51]. Consistent with the technostress creators construct, we conceptualize SRS as a second-order construct that is exhibited through its first-order subconstructs.

Coping Theory

Coping theory [38] provides a framework for understanding how employees respond to SRS. The theory describes cognitive and behavioral processes to manage psychological stress, of which SRS can be considered an example. Although coping theory is primarily concerned with an individual's response to psychological stress after it has been experienced (as opposed to the stress creation process described in the transaction-based model of stress [37]), the cognitive appraisal of stress is the first step in the coping process. Coping theory holds that individuals go through two interrelated forms of appraisal—primary and secondary—in determining whether a particular situation is stressful. In primary appraisal, the person evaluates the relevance of a situation and whether it is benign or stressful. Stressful situations are those appraised as harmful, threatening, or challenging. In secondary appraisal, the person evaluates his/her control over the stressful situation. Despite their names, primary and secondary appraisals often operate in unison [38]. Hence, we consider SRS an outcome of combined primary and secondary appraisal processes.

The combination of primary and secondary appraisals gives rise to coping efforts that aim to alleviate the felt stress. Although many classifications of coping exist in the literature [38, 48], the most widely used distinction is between problem-focused and emotion-focused coping. Problem-focused coping involves direct efforts to manage or alter the stressful situation. In the work context, these efforts can include eliminating obstacles that impede workflow or engaging in activities to increase one's knowledge and skills. Emotion-focused coping involves changing the way one thinks or feels about the stressful situation. This form of coping is inward focused and involves cognitive processes (e.g., reappraisals, distorting reality) directed at reducing emotional distress. Emotion-focused coping is more likely when there has been an appraisal that little or nothing can be done to modify the stressful situation (i.e., low controllability), whereas problem-focused coping is more probable when stressful situations are appraised as amenable to change (i.e., high controllability) [37, 38].

In couching SRS and its associated user response within coping theory, we augment the stress literature with research that considers user adaptation strategies when faced with significant IT events (e.g., technological change). User adaptation

is similar to the concept of coping, and thus IS researchers have drawn upon coping perspectives [30, 45] or used coping theory directly [11, 23, 41] to understand the process of user adaptation to different IT-related phenomena. This literature identifies several coping strategies, including mental relaxation techniques, modifying work tasks, and reinventing and adapting the technology, which generally fit within the problem- and emotion-focused categories described earlier. Pertinent to our study, user adaptation research indicates that when the expected consequences of an IT event are appraised as a threat of personal or professional relevance, and users feel that they have limited control over the situation, their adaptation efforts will be mainly emotion-focused [11, 41].

An employee's appraisal of the conditions that lead to SRS should reveal similar characteristics. That is, when experiencing SRS, employees will perceive the overload, complexity, and uncertainty of security requirements as a threat to their productivity or well-being at work (primary appraisal). The earlier evidence that users ascribe negative consequences (e.g., time, effort, frustration) to security requirements supports this position. Employees will also perceive little to no personal control over the stressful security requirements imposed upon them by the organization (secondary appraisal). Specifically, the time-consuming security protocols that characterize SRS overload are part and parcel an employee's job and are not experienced voluntarily [12]; in SRS-complexity situations, employees must digest complex administrative and technical security requirements or risk organizational sanctions for noncompliance [26, 64]; and in terms of SRS uncertainty, the rapid pace with which employees experience new and changing security requirements is dictated by management or external entities [14].

Coping theory and the user adaptation literature predict emotion-focused coping as the predominant coping strategy in this low-controllability stressful condition that requires user acceptance [11, 38]. This does not completely rule out problem-focused coping in response to SRS. Indeed, some employees may complain to management about unreasonable security requirements or update their security knowledge and skills through education and training. However, a considerable body of empirical research (e.g., [25, 39, 47, 49]) indicates that individuals rely primarily on emotion-focused coping, at least in the short term, in response to stressful organizational conditions that are not immediately amenable to change. Hence, in this study we restrict our focus to emotion-focused coping in response to SRS.

The stress literature describes emotion-focused coping in terms of a wide variety of cognitive processes directed at reducing emotional distress. Examples of these efforts include viewing stressful events in a positive light, detaching oneself from the situation, and minimizing its significance [37, 38]. Similar descriptions of emotion-focused coping include cognitive avoidance, reinterpretation, and rationalizations [17, 39, 48]. Beyond these general descriptions, there is little guidance in terms of the specific forms of emotion-focused coping and how they are linked to specific antecedents. Moreover, the various descriptions of emotion-focused coping are presented in a fairly nonintegrated way. To address these issues in our study, we draw upon moral disengagement theory (MDT) [6]. Not only do several of the MDT mechanisms parallel

the descriptions of emotion-focused coping strategies found in the stress literature, but MDT also provides a detailed and thorough account of cognitive disengagement processes within a cohesive theoretical framework. Given this conceptual similarity, we view MDT as a means to extend and enhance the description of emotion-focused coping brought forth in coping theory, and in terms of our study, provide a nuanced understanding of an emotion-focused coping response to SRS.

Moral Disengagement Theory

Research has shown that negative work stressors predict undesirable employee behaviors such as counterproductivity and deviance (e.g., [25, 57]). In this regard, employees may rationalize their undesirable behavior based on the existence of stressful work conditions. MDT provides a useful theoretical lens for describing this rationalization process. Grounded in social cognitive theory [5], MDT provides eight interrelated cognitive mechanisms, conceptualized as three broad categories (reconstruing the conduct, obscuring or distorting consequences, devaluing the target), that allow individuals to disengage the internal self-sanctions that govern their behavior [6]. Table 1 describes the MDT mechanisms along with their potential application to the ISP violation context.

MDT has been used to explain why individuals engage in inappropriate and delinquent behaviors when they understand it wrong to do so [44]. The theory has also been used to understand the cognitions that underlie self-serving behavior that is not necessarily deemed as immoral or unethical by its perpetrators, such as social loafing [2], undermining of colleagues [22], cheating [21, 59], and computer hacking [73]. According to Bandura [6], people routinely invoke moral disengagement mechanisms in everyday decisions as a means of furthering their own interests.

There is also a basis for moral disengagement as a coping mechanism. In particular, there is conceptual overlap between the general descriptions of emotion-focused coping in the stress literature and the mechanisms of moral disengagement as articulated in MDT. Emotion-focused coping processes such as positive comparison (e.g., comparing one's situation with others' that are worse), situation redefinition, and rationalization (e.g., ascribing positive value to the situation) are comparable to themes in MDT's reconstruing the conduct category; emotion-focused coping in the form of minimization of consequences, detaching oneself from the situation, and distortion of reality embody principles similar to MDT's obscuring or distorting consequences category; and emotion-focused coping processes such as blaming others and devaluing the situation are similar to descriptions of MDT's devaluing the target category. In providing these comparisons, we note that emotion-focused coping is framed in terms of the stressor itself (e.g., my situation is not as bad as someone else's), whereas moral disengagement is framed in terms of one's behavior (e.g., my policy violation is not as bad as someone else's). In a general sense, however, the concepts are quite similar and in applying these concepts moral disengagement serves a main function of emotion-focused coping, namely, attending to internal distress by means of cognitive maneuvers.

Table 1. Moral Disengagement Mechanisms

Category	Mechanism	General description	IS security policy context
Reconstruing the conduct	Moral justification	Reconstructing harmful conduct as personally and socially acceptable by portraying it as serving worthy or moral purposes; that is, service of a greater good.	Employees may justify an ISP violation in the name of getting the job done more efficiently or meeting a particular deadline, whether it is for personal accomplishment or because they feel they are doing a service to the organization.
	Euphemistic labeling	Relabeling harmful conduct through sanitized or convoluted language or concepts to make it sound benign. For example, terrorists label themselves "freedom fighters" and in the business context laying people off is referred to as "downsizing."	Employees may euphemistically label certain ISP violations as "no big deal," not such a bad thing, or an inevitable reality in the workplace.
	Palliative comparison	Considering harmful acts as acceptable by contrasting them with more reprehensible behaviors.	Employees may justify a seemingly innocuous ISP violation such as password sharing or failing to logoff a workstation by comparing it to a more severe policy violation such as stealing company information.

(continues)

Table 1. Continued

Category	Mechanism	General description	IS security policy context
Obscuring or distorting consequences	Displacement of responsibility	Viewing harmful acts as stemming from the social pressures or dictates of authority rather than being one's own responsibility.	Employees may deny responsibility for an ISP violation due to perceived work overload or a lack of alternative methods for getting the job done (both of which are the fault of management).
	Diffusion of responsibility	Diffusing responsibility across a collective (i.e., division of labor) rather than holding oneself personally accountable for harmful conduct.	Employees may perceive management, the IT department, or other employees as more responsible for IS security than themselves. An employee may also perceive that other employees are violating policy, which limits his/her overall responsibility for security.
	Distortion of consequences	Cognitive efforts to ignore, minimize, or distort the harmful consequences of one's actions.	Employees may distort the consequences of ISP violations by deeming them as not hurting the organization, at least not directly. This is plausible given that the negative effects of many ISP violations are often not directly seen or experienced by employees.
Devaluing the target	Dehumanization	Divesting the target(s) or victim(s) of harmful conduct of human qualities.	Harm resulting from an ISP violation primarily affects the organization (and not humans), and so violations may occur if employees view the company as bureaucratic, lacking emotions, or not being people oriented.
	Attribution of blame	Ascribing harmful conduct to compelling circumstances outside of one's control, such as the environment or surroundings, rather than a personal decision.	Employees may attribute ISP violations to the strictness or unreasonable nature of policies.

Within social cognitive theory [5], Bandura explicitly discusses the concept of emotion-focused coping in terms of moral disengagement mechanisms that cognitively restructure the meaning of a stressful situation. Hence, there appears to be a theoretical linkage between the emotion-focused aspect of coping theory and MDT. The question remains as to *how* moral disengagement can serve as emotion-focused coping, particularly in the organizational context. On this point, research suggests that negative work stressors, including certain technology characteristics and aspects of the IS environment, produce strain on employees (e.g., anxiety, cognitive fatigue, frustration, job dissatisfaction) and foster negative emotions and negative affect [4, 39, 49, 56, 57]. Drawing on the state instantiation of moral disengagement that is triggered by specific contextual factors [6, 44],[4] moral disengagement can be enacted in an attempt to restore emotional stability and reduce the tensions emanating from stressful work conditions. In this sense, moral disengagement can serve as an instrumental coping function that mitigates the negative effects of workplace stress on subsequent strain. Moral disengagement may also be motivated by a desire to cope with uncontrollable stressors in the work environment (e.g., SRS) such that MDT's cognitive rationalizations allow employees to assert and regain a degree of psychological control.

There is theoretical and empirical evidence to support these assertions, along with evidence that moral disengagement may not always be a deliberate coping response. For instance, situational pressures in the workplace have been theorized to increase moral disengagement [9]. Research indicates that in high-uncertainty work environments, individuals may downplay the ethical implications of a decision; the busier and more rushed employees are, the fewer cognitive resources they have to think through ethical implications of a decision [10]. Consistent with this view, cognitive psychology research provides evidence that moral values can be compromised when individuals are under psychological stress [58, 59]. Studies in both laboratory and work settings also suggest that cognitive fatigue evokes unethical behavior [8]. Hence, certain stressful work conditions appear to facilitate moral disengagement, perhaps even subconsciously. The preceding discussion supports moral disengagement as a coping mechanism, and in terms of our research model, provides a basis for moral disengagement as an emotion-focused coping response to SRS.[5] We further elaborate this relationship—in terms of our specific SRS dimensions influencing the three broad MDT categories as they relate to ISP violations—in the next section.

Research Model and Hypotheses

GROUNDED IN THE OVERARCHING FRAMEWORK OF COPING THEORY and drawing from MDT, we propose the model of the influence of SRS on employees' deliberate ISP violations in Figure 1. The model constructs and associated hypotheses are discussed next.

ISP Violation Intention

The primary outcome variable in workplace stress studies has been a measure of employee performance. In our security-related context, this performance measure is

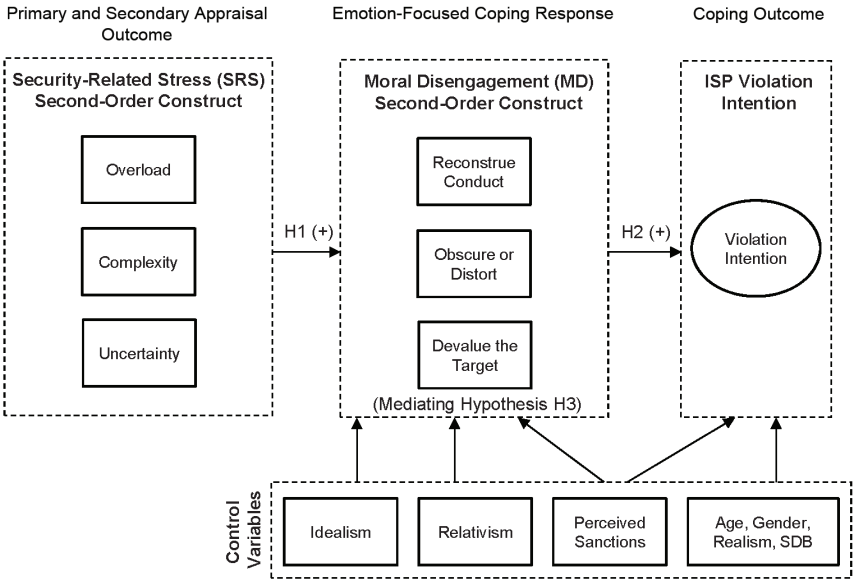

Figure 1. Research Model

ISP violations. An ISP is "a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organization" [13, pp. 526–527]. An ISP violation is therefore any act by an employee that is against the established ISP of the organization [32]. For purposes of this study, we focus on ISP violation intention instead of actual behavior. This is consistent with extant security compliance research (e.g., [20, 61]) and is partially driven by the difficulties in obtaining actual policy violation instances. Organizations are often reluctant to disclose this information to researchers [18]; furthermore, many ISP violations are not readily observable or objectively measurable [27]. We do not consider intention as a direct proxy for behavior, but instead, as a measure of a motivational state just prior to committing an act. Viewing ISP intention in this manner is consistent with workplace stress research (e.g., [39]) that considers motivation (toward a particular behavior of interest) an outcome of the coping process.

Security-Related Stress and Moral Disengagement

Turning to the relationship between SRS and moral disengagement in our model, our earlier rationale for moral disengagement as an emotion-focused coping response supports this linkage in a general sense. We now draw upon those ideas and elucidate more specific relationships that encompass the overload, complexity, and uncertainty dimensions of SRS and the three broad MDT categories as they relate to ISP violations. The first MDT category is cognitive reconstrual of the conduct itself and includes moral justification, use of euphemistic language, and palliative comparison

as specific mechanisms. Numerous, complex, and uncertain security requirements create ambiguity regarding what is and what is not acceptable user conduct. Due to this ambiguity, employees might view an ISP violation as falling within the "gray areas" of security requirements, thereby enabling positive reconstrual of the behavior in terms of euphemistic labeling (e.g., password sharing is not that bad and can make collaboration more efficient) and palliative comparisons (e.g., password sharing is minor compared to other violations). In support of this reasoning, previous research has shown that when moral or legal acceptability of a particular behavior is not clear-cut, people often categorize their own actions in positive terms [10]. Employees might also respond to SRS with attempts at restoring psychological control; given that ISP violations are often beneficial to employees, plausible mechanisms in this regard include reconstruing an ISP violation as serving an acceptable purpose (e.g., not logging off a computer or taking home sensitive data promotes productivity, password sharing helps a colleague whose access is not working), relabeling it as benign, and comparing one's own violation with more severe violations. Research also indicates that downward social comparisons (i.e., someone else is worse off than me) are common coping responses to psychological stress [37, 38]. SRS may engender an analogous response in that employees justify their own ISP violation by comparing it to others' more reprehensible violations. Based on principles of ego depletion and conservation of resources [8, 31], the existence of numerous, complex, and uncertain security requirements should decrease self-regulatory resources available to engage moral standards regarding appropriate IS behavior. This makes it likely that employees will, even inadvertently, reconstrue an ISP violation. For example, based on evidence that time pressure and uncertainty are workplace characteristics that evoke cognitive fatigue [58, 65], SRS should make it harder for employees to think through the implications of an ISP violation, thereby enabling moral justification. Moreover, because ISP violations can help employees conserve time and energy that would otherwise be exerted to comply with these policies, the positive outcomes of such violations are likely to be salient and facilitate moral justification. In light of SRS, employees might also attempt to reduce the dissonance associated with their cognitive overload by euphemistically labeling an ISP violation in benign terms or comparing it with more deleterious wrongdoings.

A second MDT category is obscuring or distorting the consequences of harmful behavior, and includes the displacement of responsibility, diffusion of responsibility, and distortion of consequences mechanisms. Overload, complexity, and uncertainty, in their own ways, make it difficult for employees to understand the value of information security, and therefore easier to diminish its importance to the organization. In particular, an abundance of complex and rapidly changing security requirements creates ambiguity about the importance of policies and how employees should view these policies as ultimately contributing to organizational efforts and protecting organizational interests. This ambiguity should make it easier for employees to divest themselves of personal accountability for security, and thus more likely to diffuse responsibility for an ISP violation. It is also easier to downplay or distort

consequences when one experiences ambiguity about what the consequences of such behaviors entail or how frequently consequences occur. Hence, conditions of SRS may allow employees to downplay the consequences of an ISP violation and justify it on these grounds. Furthermore, as the overload and complexity dimensions of SRS entail workload pressures and time constraints, employees may deny responsibility for an ISP violation for reasons of no time to comply or lack of alternative methods for meeting deadlines.

The last MDT category is devaluing the target, and includes dehumanizing and attributing blame to victims as cognitive disengagement mechanisms. Security requirements that are perceived as an overload, complex, and uncertain should produce strain in employees and negative emotional and affective reactions insofar as employees blame the organization for these negative consequences (which is likely because security requirements are levied by the organization). Consequently, employees may devalue the organization, as a whole or in terms of how it manages information security, and justify an ISP violation on such grounds (e.g., my organization is bureaucratic and not employee friendly). Employees may also use the complexity and uncertainty of security requirements to rationalize that the organization itself does not particularly value security, because if it did, ISPs would be easier to follow and less volatile. Hence, in this sense, employees can rationalize that employers bring the violations upon themselves. Furthermore, employees may construe an abundance of security requirements, and to some extent complex and uncertain security requirements, as a signal of mistrust in their competence and integrity, thereby engendering a more estranged and dehumanized relationship. Given that self-regulatory resources for harmful conduct depend partly on how the recipients are viewed [6], employees' impersonal relationship with their organization may facilitate justification of an ISP violation. Supporting this notion is research that linked intrusive formal controls (i.e., policies and monitoring mechanisms) to decreased employee trust in their organization and cooperation with an organizational policy [15].

As evident from the above discussion, there are similarities in the conceptual rationale supporting the linkages between the SRS dimensions and each of the MDT categories. Hence, it is likely that as SRS gives rise to one set of disengagement mechanisms, another set will be triggered. Moreover, one set of disengagement mechanisms likely serves to enable another. This reasoning is consistent with moral disengagement as an overall cognitive orientation consisting of three broad categories of interrelated, yet distinct, disengagement mechanisms that work to weaken self-sanctions [6]. Technostress research similarly suggests that the overload, complexity, and uncertainty dimensions operate in a collective manner [56]. Although we recognize potential relationships between the individual SRS dimensions and the MDT categories, and later call for future research that explores such relationships, consistent with our second-order conceptualizations of SRS and moral disengagement (further described in the Methodology section) and with the level of theoretical abstraction in our model, we hypothesize the following:

Hypothesis 1: SRS will be positively associated with moral disengagement from ISP violations.

Moral Disengagement and ISP Violation Intention

MDT proposes that self-sanctions that regulate illicit conduct can be deactivated through the cognitive mechanisms categorized in Table 1. As discussed, MDT has been shown to predict a variety of inappropriate/delinquent behaviors, some of which may not be unequivocally considered immoral or unethical in the mind of the perpetrator. Pertinent to our study, research has found that moral disengagement is positively associated with undesirable, self-serving behaviors in the workplace [22, 44] and security-related behaviors such as hacking [73]. Based on this theoretical and empirical evidence, moral disengagement should be relevant in the ISP violation context. In particular, positively reconstruing an ISP violation, obscuring or distorting its consequences, and devaluing the target of the violation (i.e., the organization) should contribute to increased ISP violation intention. Hence, we hypothesize the following:

Hypothesis 2: Moral disengagement from ISP violations will be positively associated with ISP violation intention.

Prior research has shown that moral disengagement mediates the relationship between individual differences and inappropriate/delinquent behavior [21]. However, the mechanisms that underlie the relationships between workplace contextual factors and illicit behavior have received less attention. Here we focus on a relation between SRS and ISP violation intention and theorize that this relationship can be explained, in part, through moral disengagement from ISP violations. Formally, we hypothesize a mediating role of moral disengagement in our model as follows:

Hypothesis 3: Moral disengagement from ISP violations will mediate the relationship between SRS and ISP violation intention.

Additional Relationships

To facilitate a more accurate assessment of our coping-based theoretical relationships, we include several control variables in our model. First, drawing on relevant literature (e.g., [13, 61]), we control for the influence of age, gender, and industry on ISP violation intention. We also include a social desirability bias control variable to help partial out potentially socially desirable responses in our results.

We also account for the influence of perceived sanctions via two relationships. Certain IS security studies support the deterrent influence of sanctions on security compliance decisions (e.g., [14, 29, 40]). We note that when Siponen and Vance [61] included sanctions together with neutralization techniques in their model of ISP violation intention, the influence of sanctions was not significant. However, consistent with deterrence theory, and for purposes of nomological validity, we include a relationship between perceived sanctions and ISP violation intention. We also include a relationship between perceived sanctions and moral disengagement. This is based on the theoretical position that formal sanctions discourage the dissociation of harmful acts from self-evaluative consequences [5, 68] and empirical research that affirms this phenomenon in the

organizational context [19, 46]. Hence, the presence of sanctions for an ISP violation should decrease an employee's ability to rationalize and justify such behavior.

Lastly, an individual difference variable with strong ties to moral disengagement is ethical orientation and, following Moore et al.'s [44] recommendation, we control for this relationship in our model. Empirical studies have linked the idealism/relativism ethical orientation dimensions to a variety of unethical organizational behaviors (see [35, 44]). Accordingly, we expect that idealism will have a negative relationship with moral disengagement because idealists pursue absolute ethical standards and therefore are less likely to subvert their personal codes of conduct. Conversely, we expect a positive relationship between relativism and moral disengagement because relativists are more likely to justify ISP violations based on circumstances (i.e., situational ethics) and this is facilitated by morally disengaged cognitions.

Methodology

Scenarios

This study utilized an online survey instrument for data collection. The survey first presented respondents with one of five randomly selected scenarios describing an ISP violation. We developed our five ISP violation scenarios in multiple phases based on guidelines for IS security field surveys [62]. First, after reviewing industry surveys and the IS security literature, we identified password sharing, password write-down, copying sensitive data to an insecure USB device, and failure to logoff workstation as common and significant ISP violations. We adapted existing scenarios depicting these behaviors for our study [27, 61]. Next, to ensure that our choice of ISP violations was relevant to practice, we conducted interviews with six IS security practitioners. Each identified the four aforementioned ISP violations as major security compliance problems in addition to another important security issue: data leakage. Hence, we developed an original ISP violation scenario depicting data leakage. The practitioners along with four IS faculty members were then asked to comment on the wording and realism of each scenario, which resulted in some modifications. To ensure relevance to ordinary users, we asked survey respondents to rate each scenario's realism (1 = "highly unrealistic" to 7 = "highly realistic") and we used this measure as an additional control variable in the analysis. The mean realism score for each scenario was at least 4.3, which provides reasonable assurance that the scenarios were realistic and broadly applicable to business settings.

Measures

Following the scenario, respondents received a series of questions designed to measure moral disengagement (MD), perceived sanctions (PS), and intention (INT) as each related to the ISP violation depicted in the scenario. INT was measured with two items adapted from D'Arcy et al. [20];[6] PS was measured with six items adapted from Hu et al. [32] and Siponen and Vance [61] that tapped into the certainty, severity, and

celerity dimensions of PS.[7] MD items were taken from Bandura et al.'s [7] 32-item scale but reworded and adapted for our ISP violation context. Since this scale was not originally developed for the organizational context, some of the items seemed out of place for our study, even after they were reworded. After careful analysis, we ended up with three items for each of the MD dimensions (24 total items). Other researchers have employed a similar approach in selecting only relevant items in adapting this scale to a new context [21, 59]. Consistent with MD as an overall cognitive orientation consisting of three broad categories [6], and following recent empirical work [22], we conceptualized MD as a second-order construct consisting of its three broad categories as first-order subconstructs.

After the scenario-specific items, a separate section of the survey measured SRS, ethical orientation, and social desirability bias (SDB). Similar to the MD items, we adapted the SRS items from their technostress creators counterparts [56]. In some cases the technostress creators items did not translate to the security context, so not all items were adapted. Our SRS measure consisted of 14 items that tapped into the SRS-overload (four items), SRS-complexity (six items), and SRS-uncertainty (four items) dimensions. Ethical orientation was measured with Forsyth's [24] ethics position questionnaire, which contains 10 items for idealism and 10 items for relativism. SDB was measured with a five-item subset of the Marlowe–Crowne social desirability response scale [28]. This scale measures an individual's tendency to behave in a culturally appropriate and acceptable manner. The full list of survey items is in Appendix A.

We reviewed our measures using criteria for formative and reflective constructs [34, 43] and determined that all of the first-order constructs were reflective. Consistent with the technostress creators construct, we modeled SRS as reflectively composed of its subconstructs (i.e., a reflective first-order, reflective second-order construct). As suggested by an anonymous reviewer, a rationale is that each SRS dimension by itself can create stress and one need not experience the presence of all three dimensions to experience SRS. Similarly, following the description of MD as a set of interrelated dimensions that are manifestations of an overarching concept [6], and consistent with recent empirical studies that consider these dimensions in a mutually reinforcing manner [21, 22, 59], we modeled MD as a reflective first-order, reflective second-order construct.

Sample

We used a market research firm to invite participants to take our survey. External panelists have been used increasingly in IS research (e.g., [4, 13, 51]) and have certain advantages over traditional methods that were key to our study. First, panels guarantee respondent anonymity and thereby encourage honest responses to questions that may be subject to socially desirable responses. Second, external panels contain respondents from a wide range of industries and positions who would be difficult to obtain otherwise. This sample heterogeneity reduces potential bias due to unique organizational factors [13].

We instructed the marketing research firm to collect responses from employed, computer-using professionals. The research firm paid participants a small amount for their participation. According to available statistics, 1,194 panel members accepted the invitation to participate in the survey by viewing the consent agreement and clicking past the first page. We eliminated 655 respondents due to missing data or nonconscientious responding (i.e., answers exhibiting certain unlikely patterns, such as all 7 or alternating 6 and 7, or survey completed in an unreasonably short time). The percentage of eliminated respondents is consistent with other studies that utilized external panelists [4, 13, 51]. The final sample consisted of 539 usable responses (see Appendix B). We checked for possible nonresponse bias and found no significant differences between the first third and last third of the data, nor were the usable responses significantly different from those that were eliminated based on several demographic characteristics. Hence, we concluded that nonresponse bias was not a serious problem.

Analysis and Results

We used SmartPLS (version 2.0) as the primary statistical tool to analyze the measurement and structural models. Partial least squares (PLS) is well suited for the predictive nature of our study, and allowed us to assess the relative influences of SRS and MD in our model in a manner similar to hierarchical regression. We augmented our PLS analysis with a covariance-based factor-analytic procedure using EQS (version 6.2).

Measurement Model

Supporting details of the measurement model analysis, including tests for common method variance, are provided in a supplemental online appendix available on the first author's Web site (http://sites.udel.edu/jdarcy/research/). We summarize these tests and their results here. First, as all first-order constructs were reflective, we assessed their measurement adequacy through conventional tests of convergent validity, reliability, and discriminant validity [43]. For convergent validity, all factor loadings should exceed 0.70 and the average variance extracted (AVE) for each construct should exceed 0.50. After removal of certain items with poor loadings or cross-loadings, both criteria were met for all constructs. Further evidence of the convergent validity of all remaining items comes from their significant *t*-statistics. Reliability was assessed using Cronbach's alpha and composite reliability scores, with the recommended threshold of 0.70 being met for all constructs.

For discriminant validity, the square root of the AVE for each construct should be larger than the interconstruct correlations, and items should load more strongly on their corresponding construct than on other constructs (i.e., at least 0.10 higher than cross-loadings). These conditions were met for all constructs with the exception of MD. Several MD items cross-loaded and there were high correlations (albeit within the 0.90 cutoff [43]) among the first-order MD constructs. However, the aforementioned covariance-based factor-analytic procedure (detailed in the supplemental online appendix) supported the discriminant validity of the first-order MD constructs and

provided justification for MD as a reflective second-order construct consisting of three distinct first-order subconstructs.

Following proscribed procedures [43], we also calculated the AVE for each second-order construct by averaging the square of each first-order subdimension's standardized loading on the second-order construct. AVE values greater than 0.50 indicate that, on average, a majority of the variance in the first-order dimensions is shared with the second-order construct. The AVE values for SRS and MD were 0.70 and 0.85, respectively, which are both above the recommended threshold.

In addition, and furthering our assessment of discriminant validity, we included the moral belief (MB) construct in our measurement model analysis (see Appendix A for MB items). Our intention was to determine whether one's moral belief regarding an ISP violation is distinct from his or her moral disengagement from the behavior. We felt it important to distinguish MB from MD because the two constructs are conceptually related and MB has been used in prior security compliance studies (e.g., [33, 40]). The results support the distinctiveness of the MB and MD constructs, as MB did not cross-load on any of the MD dimensions and the square root of MB's AVE was higher than that of its interconstruct correlations. We also ran a structural model with an added path between MB and INT; there was no substantive change in the original path coefficients. Finally, we assessed the potential for common method variance in our results using contemporary procedures [43, 50] and found no serious cause for concern.

Structural Model

The hypotheses were tested by examining the structural model. Bootstrapping (600 resamples) was used to determine the significance of the path coefficients. The second-order SRS and MD constructs were estimated using the factor scores of their first-order dimensions as reflective indicators (see [72]). The structural model results are shown in Figure 2.

The model explained approximately 46 percent of the variance in INT and approximately 44 percent of the variance in MD. SRS had a significant positive relationship with MD ($\beta = 0.358$, $p < 0.001$), thereby supporting H1. MD likewise had a significant positive relationship with INT ($\beta = 0.528$, $p < 0.001$), thereby supporting H2. In terms of the control variables, the direct relationship between PS and INT was not supported; however, PS had a significant negative relationship with MD ($\beta = -0.498$, $p < 0.001$). Relativism also had a significant positive relationship with INT ($\beta = 0.141$, $p < 0.01$), but the predicted relationship between idealism and INT was not supported. Scenario realism ($\beta = 0.236$, $p < 0.001$) was the only other significant control variable. Of note is the nonsignificance of SDB, which helps allay concerns of socially desirable responses in our results.

We also assessed the relative contributions of SRS and MD beyond that of PS, ethical orientation, and the other control variables. A model with only PS and the control variables explained 29 percent of the variance in INT, a 17 percent decrease from when MD was included. This change in R^2 represents a medium to large effect size (0.31) that is significant ($p < 0.001$) based on a pseudo F-test (e.g., [61]). Next, we removed

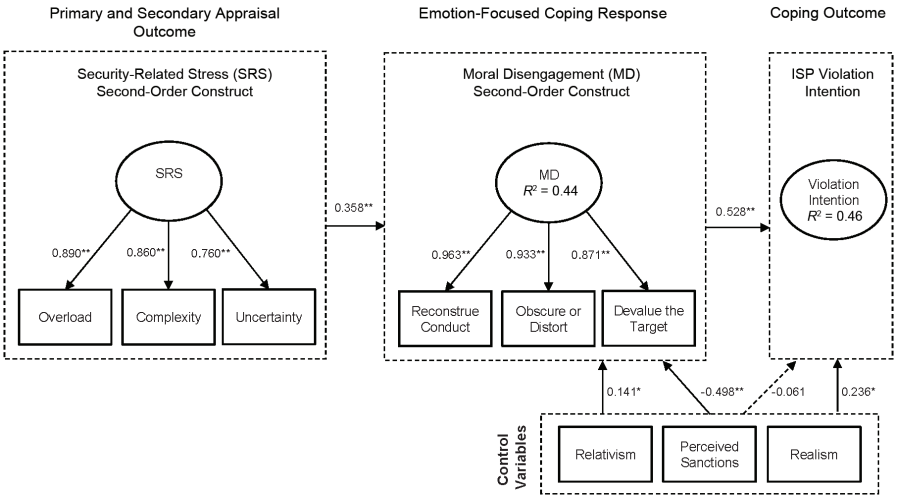

Figure 2. Structural Model Results

Notes: Paths in dash are not significant ($p > 0.05$). Nonsignificant control variables are not shown. * $p < 0.01$; ** $p < 0.001$.

SRS from the final model so that PS, idealism, and relativism were the only predictors of MD. The R^2 for MD decreased from 44 percent to 32 percent, representing a medium effect size (0.21) that is also significant ($p < 0.001$). These results support the substantive influences of SRS and MD in our model beyond that of PS, ethical orientation, and the other control variables.

To test H3, we conducted a Sobel test, which is a method for assessing indirect effects that is considered superior (i.e., better balance between Type 1 and Type II errors) to the traditional Baron–Kenny mediation test when using larger sample sizes [21]. We conducted the Sobel test for the indirect effect of SRS on INT through MD using Preacher's online Sobel test calculator (http://quantpsy.org/sobel/sobel.htm). The Sobel test statistics were significant ($z = 7.98$, $p < 0.001$), thereby supporting H3 and suggesting that MD plays a mediating role between SRS and INT.

We also ran five scenario-specific models to determine whether the results reported in Figure 2 are consistent across the individual scenarios. We emphasize that these results should be interpreted with caution given their lower sample sizes (average $n = 108$ over the five models). For each scenario, the hypothesized paths had nearly the same magnitude, with the same sign and significance as those in Figure 2 with the following exception: The path from PS to MD dipped just below significance ($p > 0.05$) for the password write-down scenario.

Discussion and Contributions

OUR RESULTS PROVIDE EVIDENCE THAT CONDITIONS OF SRS—in the form of security requirements that are perceived as an overload, complex, and uncertain—can induce moral

disengagement from ISP policy violations, which in turn make one more susceptible to this behavior. Hence, SRS and moral disengagement are key factors that predict employees' ISP violations, beyond the influences of deterrence-based sanctions and ethical orientation. The influence of SRS in our model is noteworthy because it points to a potential negative influence of security requirements on user behavior, a topic that has received scant attention in the IS literature. This finding also underscores the role of contextual workplace factors in security compliance decisions, an area that has received less research attention compared to purely person-related factors (i.e., attitudes, beliefs, and dispositions) that are not embedded in the social context of the workplace. Through SRS, we add a new conceptual dimension to the sizable research that has explored the determinants of security policy compliance.

Consistent with organizational stress research that supports a relationship between negative work stressors and undesirable employee behaviors, we found evidence of a linkage between SRS and ISP-violating behavior. However, as a departure from extant work we did not focus solely on job-related strains (e.g., anxiety, emotional exhaustion, job satisfaction, organizational commitment) caused by work stressors. Instead, we drew from coping theory and MDT and found that an underlying mechanism through which SRS influences employee behavior is emotion-focused coping in the form of moral disengagement from ISP violations. Moral disengagement provides a coping response to SRS by allowing employees to rationalize their ISP-violating behavior. This rationalization occurs through cognitive mechanisms that center on positive reconstrual of the ISP violation, obscuring or distorting its consequences, and devaluing the target of the violation (i.e., organization). Our results are similar to MDT applications in other contexts in explaining how otherwise decent people can knowingly engage in illicit behavior without apparent guilt or self-censure. In this sense, our study provides a theoretical explanation for industry findings that a majority of ISP violations are committed by well-meaning employees without malicious intent [69].

Our findings are also consistent with Siponen and Vance's [61] research that found neutralization techniques as predictors of ISP violations. We complement and extend this work with a different set of cognitive rationalization processes that are rooted in social cognitive theory and with a more nuanced measurement approach that is specific to our scenario behaviors. More importantly, we provide and empirically validate a set of antecedents rooted in the workplace stress and technostress literature that can inspire cognitive rationalizations and justifications that lead to ISP violations. By doing so, we heed the call for research on the situations that evoke rationalization techniques in the IS security domain [71].

Our study extends technostress research that has identified technology characteristics and their relation to stressors and the outcomes of technostress. We broaden the reach of this work from the technology itself to stress arising from the security-related policies, procedures, and technical controls of the organization, its coping process, and to new outcomes in the form of ISP violations. Furthermore, unlike extant technostress research, we explicitly examine the coping mechanisms that underlie an employee's reaction to stressful workplace situations.

Our study also explored the role of sanctions in security compliance decisions. Contrary to our expectations and the predictions of deterrence theory, we did not find support for a direct relationship between perceived sanctions and ISP intention. This finding is inconsistent with some security compliance studies [14, 29, 40], although others have reported that sanctions did not influence policy noncompliance [27, 33, 61]. In Siponen and Vance's [61] study of employee neutralization of ISP violations, the authors found that sanctions became nonsignificant once neutralization constructs were added to their model. We performed a similar analysis and found that the effect of sanctions was significant ($p < 0.05$) in a simplified model that did not include moral disengagement; adding moral disengagement to the model reduced the effect of sanctions to nonsignificance. Our results corroborate Siponen and Vance's in demonstrating that cognitive rationalizations are much stronger direct predictors of ISP violations than are sanctions. However, unlike Siponen and Vance, we provide evidence that the influence of sanctions is not irrelevant in security compliance decisions even when rationalizations are taken into account. Our significant relationship between sanctions and moral disengagement supports the position that sanctions articulate the moral stance of the organization, which reduces employees' propensity to morally disengage and their subsequent ISP-violating behavior.

Practical Implications

This study provides insights into the phenomenon of ISP violations that have practical relevance. We found evidence that when employees perceive stress due to security requirements, they are more likely to rationalize ISP violations through moral disengagement, resulting in an increased susceptibility toward violating behavior. Hence, organizations need to engage in efforts to detect and counter SRS. In terms of detection, we identified specific organizational conditions—namely, security-related overload, complexity, and uncertainty—that signify the existence of SRS among employees. Managers can use the items provided in Appendix A as a diagnostic tool to evaluate the presence of SRS in their organizations. Our findings also point to potential mechanisms to reduce SRS. Perhaps the most obvious are precise and clearly written (i.e., devoid of excessive technical jargon and legal terms) security policies that contain detailed compliance procedures. Such policies should help alleviate the perceived complexity of security requirements, particularly for nontechnical staff. Organizations can also combat security-related complexity with periodic security education, training, and awareness (SETA) programs that convey the latest security knowledge and technical skills. In an effort to reduce uncertainty toward security requirements, SETA programs can include a component that describes the current regulatory landscape and upcoming security policy changes (administrative and technical) so that employees can prepare to assimilate them into their work routines. Organizations can also involve employees in the design and implementation of security requirements as a means to reduce SRS. Examples include testing of new security requirements, providing feedback to management, and communicating security changes to coworkers [53, 63]. Involving employees in this manner should reduce uncertainty because employees will be bet-

ter informed as to why new security requirements are occurring; complexity should also be reduced because employees will have had an opportunity to familiarize themselves with security requirements before they are fully implemented; furthermore, having some influence over the design and implementation of security requirements, employees should perceive the requirements as less offsetting to productivity, which should reduce feelings of overload. Additional mechanisms for countering overload can include responsive technical support (e.g., handling password issues in a timely manner) and user-friendly software solutions (e.g., single sign-on authentication) that streamline security requirements.

In addition to dealing with stress related to security requirements, organizations need to make a concerted effort to ward off cognitive rationalization mechanisms that evoke ISP violations. Our results suggest that formal sanctions are an effective mechanism in this regard. Beyond providing an important normative foundation and basis for punishment for would-be offenders, formal sanctions convey that ISP violations are incongruent with the organization's moral stance. Organizations should clearly articulate the certainty, severity, and swiftness of sanctions for ISP violations within security policies and SETA programs. Security policies and SETA programs should include explicit content that addresses cognitive rationalizations that center on positive reconstrual of the ISP violation, obscuring/distorting its consequences, and devaluing the target. This content should include statements that emphasize: (1) the responsibility that every employee has toward information security; (2) that ISP violations can never be justified regardless of circumstances, such as burdensome security requirements and tight deadlines; and (3) that the harm resulting from ISP violations, although not always directly seen by employees, can have dire financial and reputational consequences for the organization, and can potentially affect employees (e.g., employees' personal information can be compromised).

The study findings shed light on the types of people that are more susceptible to ISP violations. In particular, those with the relativist ethical orientation are more likely to rationalize an ISP violation. Although this individual difference is not readily observable in most individuals, organizations could look for it as part of a broader selection process using techniques such as an established ethical orientation scales (e.g., [24]).

Limitations and Future Research

IT IS IMPORTANT TO CONSIDER THE FOLLOWING LIMITATIONS TO THIS STUDY, some of which point to opportunities for future research. The first limitation is the single source for both the dependent and independent variables, which could introduce common method variance. While formal tests revealed that common method variance was not prevalent, the research would be strengthened by a longitudinal design with a lag between the collection of the dependent and independent variables or through measures of actual ISP violations obtained from independent sources.

Second, the phenomenon of ISP violations in this study is limited to more common, less extreme incidents that require minimal technical sophistication. Although we intentionally chose this route based on our literature review and feedback from

IS security practitioners, a trade-off is that our findings may not generalize to more extreme, potentially disastrous security incidents. However, as research suggests a link between minor policy violations and more serious computer abuses [69], our findings have potential implications beyond the five types of ISP violations included here.

Third, consistent with most psychological stress research, we measured SRS indirectly through a self-reported perceptual measure that assessed stress-inducing conditions. Future research can build on our initial work and utilize objective measures (e.g., physiological techniques) to gauge SRS. Future research could propose and test hypotheses between specific dimensions of our SRS construct and one or more of the three MDT categories. Exploring such relationships at the subconstruct level may reveal interesting and insightful detail regarding SRS and its coping response, and would complement our theoretical explanations and analysis at the higher (i.e., second-order) level of abstraction. Our first-order scales for SRS and MD provide a starting point for others who wish to pursue this research avenue.

Finally, future research can investigate the negative effects of SRS on factors beyond moral disengagement and ISP violations. SRS could conceivably manifest itself in emotion-focused coping (and moral disengagement in particular) related to several security-diminishing behaviors (e.g., computer abuse, IS misuse) and not just ISP violations. We positioned moral disengagement from ISP violations as one plausible coping response to SRS and focused on that in this study. Moving beyond the IS realm, the stress literature points to an array of physiological and psychological reactions to accelerating workplace demands that can be investigated as potential outcomes of SRS.

Conclusion

EMPLOYEES' DELIBERATE ISP VIOLATIONS PLAGUE ORGANIZATIONS despite increasing countermeasures, such as security policies and SETA programs, designed to thwart such behavior. One explanation for this predicament, which we explored in this study, is the stressful demands imposed by internal security requirements. Using coping theory as an overarching framework and drawing from moral disengagement theory, we hypothesized and found evidence that security requirements perceived as an overload, complex, and uncertain can induce employee rationalizations of ISP violations, which in turn increase susceptibility to this behavior. Hence, organizations need to be cognizant of the stress-creating aspects of security requirements as they work to protect their information assets from insider threats. The results of this study offer a glimpse of the potential adverse effects of security requirements on user behavior and hopefully provide motivation for future work that expands upon our research. We consider this a critical topic given the dynamically changing security environment that employees encounter in the workplace.

NOTES

1. The organizational stress literature differentiates between positive and negative work stressors, using the terms *challenge* and *hindrance stressors,* respectively. Challenge

stressors are (positive) job demands appraised as rewarding and career enhancing (e.g., increased job responsibility). Hindrance stressors are (negative) job demands appraised as impeding one's ability to achieve valued goals (e.g., work overload, administrative hassles) [17, 47].

2. To be clear, SRS does not refer to stress itself (which is a process), but rather conditions or factors that create SRS. Our conceptualization of SRS is consistent with extant definitions and operationalizations of psychological stress that consider stress in terms of stimulating conditions that produce stress reactions [37, 38]. We further describe the SRS construct, based on the technostress creators construct [56, 67], in the Security-Related Stress subsection of the paper.

3. We initially included parallel security-related constructs for the techno-invasion and techno-insecurity dimensions but omitted them for the following reasons. First, some techno-invasion and techno-insecurity items could not be reasonably adapted to the security context, or when adapted, overlapped conceptually with the newly adapted SRS-overload and SRS-complexity items. A confirmatory factor analysis supported this view empirically. Furthermore, upon viewing the adapted items, two anonymous reviewers suggested that the techno-invasion and techno-insecurity dimensions were not relevant to the security context.

4. The literature on moral disengagement identifies both trait and state instantiations of the concept [6, 44]. Moral disengagement as a trait is an individual difference that represents a generalized cognitive orientation to morally disengage across contexts. A state instantiation of moral disengagement refers to morally disengaged reasoning that is triggered by specific circumstances or contextual factors in particular contexts. We focus on a state instantiation of moral disengagement in this study, namely, moral disengagement from ISP violations that is triggered by SRS.

5. An additional point pertaining to MDT warrants attention. Within the criminology literature, there are themes comparable to moral disengagement captured within neutralization theory [66]. Neutralization theory and MDT both provide cognitive rationalizations for acting in ways that violate self-standards of behavior. Accordingly, in comparing our study to Siponen and Vance's [61] study of employee neutralization of ISP violations, several of the moral disengagement mechanisms are close analogs to their neutralization techniques. We acknowledge this theoretical congruence and emphasize that our contribution is not solely in terms of the influence of cognitive rationalization processes on ISP violations, but instead involves a set of theoretically derived workplace antecedents of these rationalization processes in the form of SRS. In a supplemental appendix to this paper (available at http://sites.udel.edu/jdarcy/research/), we provide a detailed exposition that (1) provides a theoretical rationale for using MDT as opposed to neutralization theory for this particular study, (2) summarizes the key differences between MDT and neutralization theory, and (3) distinguishes our scenario-specific moral disengagement measures from Siponen and Vance's neutralization measures that pertain to ISP violations in general.

6. Although we acknowledge the limitations of two-item measures, we believe that our two-item intention measure is adequate based on its contextual nature—that is, intention in this study relates to a particular ISP-violating behavior as depicted in the scenario. Respondents reported the likelihood of themselves engaging in the behavior via the two items immediately following the scenario. Hence, as argued by Siponen and Vance [61] in their scenario-based study, little measurement error is expected for this proximal measure. Other intention measures that consist of more than two items typically attempt to capture intention toward a more general behavior, such as technology usage, and therefore would benefit from a broader range of measurement items. We also chose the two-item intention measure for pragmatic reasons. Based on our experience in conducting scenario-based studies, respondents find multiple, similar items that relate to the scenarios to be frustrating and have expressed concerns that the researchers are trying to deceive them. We did not want to engender such negative reactions in our study, and considering that a third intention item would be semantically redundant to the other two items (given the contextual nature of the scenario), we took a conservative approach and utilized the two-item scale.

7. We considered modeling PS as a second-order construct with the three dimensions as first-order constructs, but our measurement model analysis revealed a single, six-item PS factor that exhibited strong reliability. A similar composite PS construct has been used in prior IS security studies [13, 61].

References

1. Alge, B.J. Effects of computer surveillance on perceptions of privacy and procedural justice. *Journal of Applied Psychology, 86,* 4 (2001), 797–804.

2. Alnuaimi, O.A.; Robert, L.P.; and Maruping, L.M. Team size, dispersion, and social loafing in technology-supported teams: A perspective on the theory of moral disengagement. *Journal of Management Information Systems, 27,* 1 (Summer 2010), 203–230.

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

4. Ayyagari, R.; Grover, V.; and Purvis, R. Technostress: Technological antecedents and implications. *MIS Quarterly, 35,* 4 (2011), 831–858.

5. Bandura, A. *Social Foundations of Thought and Action: A Social Cognitive Theory.* Englewood Cliffs, NJ: Prentice Hall, 1986.

6. Bandura, A. Social cognitive theory of moral thought and action. In W.M. Kurtines and J.L. Gewitz (eds.), *Handbook of Moral Behavior and Development,* vol. 1. Hillsdale, NJ: Lawrence Erlbaum, 1991, pp. 45–103.

7. Bandura, A.; Barbaranelli, C.; Caprara, G.V.; and Pastorelli, C. Mechanisms of moral disengagement in the exercise of moral agency. *Journal of Personality and Social Psychology, 71,* 2 (1996), 364–374.

8. Barnes, C.M.; Schaubroeck, J.; Huth, M.; and Ghumman, S. Lack of sleep and unethical conduct. *Organizational Behavior and Human Decision Processes, 115,* 2 (2011), 169–180.

9. Batson, C.D., and Thompson, E.R. Why don't people act morally? Motivational considerations. *Current Directions in Psychological Science, 10,* 2 (2001), 54–57.

10. Bazerman, M.H., and Tenbrunsel, A.E. *Blind Spots: Why We Fail to Do What's Right and What to Do About It.* Princeton: Princeton University Press, 2011.

11. Beaudry, A., and Pinsonneault, A. Understanding user responses to information technology: A coping model of user adaptation. *MIS Quarterly, 29,* 3 (2005), 493–524.

12. Beautement, A.; Sasse, M.A.; and Wonham, M. The compliance budget: Managing security behavior in organizations. In *Proceedings of the 2008 Workshop on New Security Paradigms.* New York: ACM Press, 2008, pp. 47–58.

13. Bulgurcu B.; Cavusoglu, H.; and Benbasat, I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34,* 3 (2010), 523–548.

14. Chen, Y.; Ramamurthy, K.; and Wen, K.-W. Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29,* 3 (Winter 2012–13), 157–188.

15. Christ, M.H.; Sedatole, K.L.; Towry, K.L.; and Thomas, M.A. When formal controls undermine trust and cooperation. *Strategic Finance, 89,* 7 (2010), 39–44.

16. Cisco Systems. 2011 Cisco connected world technology report. San Jose, CA, 2011.

17. Crawford, E.R.; LePine, J.A.; and Rich, B.L. Linking job demands and resources to employee engagement and burnout: A theoretical extension and meta-analytic test. *Journal of Applied Psychology, 95,* 5 (2010), 834–848.

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

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

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

21. Detert, J.R.; Trevino, L.K.; and Sweitzer, V.L. Moral disengagement in ethical decision making: A study of antecedents and outcomes. *Journal of Applied Psychology, 93,* 2 (2008), 374–391.

22. Duffy, M.K.; Scott, K.L.; Shaw, J.D.; Tepper, B.J.; and Aquino, K. A social context model of envy and social undermining. *Academy of Management Journal, 55,* 3 (2012), 643–666.

23. Fadel, K.J., and Brown, S.A. Information systems appraisal and coping: The role of user perceptions. *Communications of the Association for Information Systems, 26,* 6 (2010), 107–126.

24. Forsyth, D.R. A taxonomy of ethical ideologies. *Journal of Personality and Social Psychology, 39,* 1 (1980), 175–184.

25. Gilboa, S.; Shirom, A.; Fried, Y.; and Cooper, G. A meta-analysis of work demand stressors and job performance: Examining main and moderating effects. *Personnel Psychology, 61,* 2 (2008), 227–271.

26. Goel, S., and Chengalur-Smith, I.N. Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems, 19,* 4 (2010), 281–295.

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

28. Hays, R.D.; Hayashi, T.; and Stewart, A.L. A five-item measure of socially desirable response set. *Educational and Psychological Measurement, 49,* 3 (1989), 629–637.

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

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

31. Hobfoll, S.E. Conservation of resources. *American Psychologist, 44,* 3 (1989), 513–524.

32. Hu, Q.; Dinev, T.; Hart, P.; and Cooke, D. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43,* 4 (2012), 615–660.

33. Hu, Q.; Zhengchuan, X.; Dinev, T.; and Ling, H. Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54,* 6 (2011), 54–60.

34. Jarvis, C.B.; MacKenzie, S.B.; and Podsakoff, P.M. A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research, 30,* 2 (2003), 199–218.

35. Kish-Gephart, J.J.; Harrison, D.A.; and Trevino, L.K. Bad apples, bad cases, and bad barrels: Meta-analytic evidence about sources of unethical decisions at work. *Journal of Applied Psychology, 95,* 1 (2010), 1–31.

36. Kwon, J., and Johnson, M.E. Healthcare security strategies for information security and regulatory compliance. *Journal of Management Information Systems, 30,* 2 (Fall 2013), 41–66.

37. Lazarus, R.S. *Psychological Stress and the Coping Process.* New York: McGraw-Hill, 1966.

38. Lazarus, R.S., and Folkman, S. *Stress, Appraisal, and Coping.* New York: Springer, 1984.

39. LePine, J.A.; Podsakoff, N.P.; and LePine, M.A. A meta-analytic test of the challenge stressor–hindrance stressor framework: An explanation for inconsistent relationships among stressors and performance. *Journal of Applied Psychology, 48,* 5 (2005), 764–775.

40. Li, H.; Zhang, J.; and Sarathy, R. Understanding compliance with Internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48,* 4 (2010), 635–645.

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

42. Lim, V.K.G. The IT way of loafing on the job: Cyberloafing, neutralizing, and organizational justice. *Journal of Organizational Behavior, 23,* 5 (2002), 675–694.

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

44. Moore, C.; Detert, J.R.; Trevino, L.K.; Baker, V.I.; and Mayer, D.M. Why employees do bad things: Moral disengagement and unethical organizational behavior. *Personnel Psychology, 65,* 1 (2012), 1–48.

45. Nelson, D., and Kletke, M.G. Individual adjustment during technological innovation: A research framework. *Behavior and Information Technology, 9,* 4 (1995), 257–271.

46. Paternoster, R., and Simpson, S. Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review, 30,* 3 (1996), 549–584.

47. Pearsall, M.J.; Ellis, A.P.J.; and Steinm, J.H. Coping with challenge and hindrance stressors in teams: Behavioral, cognitive, and affective outcomes. *Organizational Behavior and Human Decision Processes, 109,* 1 (2009), 18–28.

48. Perrewe, P.L., and Zellars, K.L. An examination of attributions and emotions in the transactional approach to organizational stress process. *Journal of Organizational Behavior, 20,* 5 (1999), 739–752.

49. Podsakoff, N.P.; LePine, J.A.; and LePine, M.A. Differential challenge stressor–hindrance stressor relationships with job attitudes, turnover intentions, turnover, and withdrawal behavior: A meta-analysis. *Journal of Applied Psychology, 92,* 2 (2007), 438–454.

50. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.Y.; and Podsakoff, N.P. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88,* 5 (2003), 879–903.

51. Posey, C.; Bennett, R.J.; and Roberts, T.L. Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security, 30,* 6 (2011), 486–497.

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

53. Post, G.V., and Kagan, A. Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security, 26,* 3 (2007), 229–237.

54. PricewaterhouseCoopers. Global State of Information Security® survey 2013. New York, 2013.

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

56. Ragu-Nathan, T.S.; Tarafdar, M.; and Ragu-Nathan, B.S. The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information Systems Research, 19,* 4 (2008), 417–433.

57. Rodell, J.B., and Judge, T.A. Can "good" stressors spark "bad" behaviors? The mediating role of emotions in links of challenge and hindrance stressors with citizenship and counterproductive behaviors. *Journal of Applied Psychology, 94,* 6 (2009), 1438–1451.

58. Shalvi, S.; Eldar, O.; and Bereby-Meyer, Y. Honesty requires time (and lack of justifications). *Psychological Science, 23,* 10 (2012), 1264–1270.

59. Shu, L.L.; Gino, F.; and Bazerman, M.H. Dishonest deed, clear conscience: When cheating leads to moral disengagement and motivated forgetting. *Personality and Social Psychology Bulletin, 37,* 3 (2011), 330–349.

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

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

62. Siponen, M., and Vance, A. Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems, 23,* 3 (2014), 289–305.

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

64. Stanton, J.M., and Stam, K.R. *The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets—Without Compromising Employee Privacy or Trust.* Medford, NJ: Information Today, 2006.

65. Suter, R.S., and Hertwig, R. Time and moral judgment. *Cognition, 119,* 3 (2011), 454–458.

66. Sykes, G., and Matza, D. Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22,* 6 (1957), 664–670.

67. Tarafdar, M.; Tu, Q.; and Ragu-Nathan, T.S. Impact of technostress on end-user satisfaction and performance. *Journal of Management Information Systems, 27,* 3 (Winter 2010–11), 303–334.

68. von Hirsch, A.; Bottoms, A.E.; Burney, E.; and Wikstromm P.-O. *Criminal Deterrence and Sentence Severity: An Analysis of Recent Research.* Oxford: Hart, 1999.

69. Wall, D.S. Organizational security and the insider threat: Malicious, negligent, and well-meaning insiders. Symantec Research Report, Mountain View, CA, 2011.
70. Warkentin, M.; Johnston, A.C.; and Shropshire, J. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20,* 3 (2011), 267–284.
71. Willison, R., and Warkentin, M. Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37,* 1 (2013), 1–20.
72. Wright, R.T.; Campbell, D.E.; Thatcher, J.B.; and Roberts, N. Operationalizing multidimensional constructs in structural equation modeling: Recommendations for IS research. *Communications of the Association for Information Systems, 30,* 23 (2012), 367–412.
73. Young, R.; Zhang, L.; and Prybutok, V.R. Hacking into the minds of hackers. *Information Systems Management, 24,* 4 (2007), 281–287.
74. Zhao, X.; Xue, L.; and Whinston, A. Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems, 30,* 1 (Summer 2013), 123–152.

Appendix A: Scenarios and Survey Items

ISP Violation Scenarios

Password-Sharing Scenario

Jim is an employee in your organization. One day while Jim is out of the office on a sick day, one of his coworkers needs a file on Jim's computer. The coworker is of equal rank and performs job functions similar to Jim's. The coworker calls Jim and asks for the password. Although Jim knows that your organization has a policy that passwords must not be shared, he shares his password with the coworker.

Password Write-Down Scenario

Lee is an employee in your organization. The organization recently installed a computer system for managing employee personal information (e.g., employee emergency contacts, retirement benefits, salary information). Each employee has been given a user name and password for the system. Lee is aware of the company policy stating that users are required to keep their passwords to themselves and not let other people know or use them. However, finding it difficult to remember his password, Lee wrote it down on a sticky note and attached it to the computer he usually uses.

Failure to Logoff Scenario

Pat is an employee in your organization. As part of his job, Pat has been given authorized access to the company's payroll system. One day at work, Pat logs into the payroll system to gather information for a weekly report that he prepares for management. After some time, Pat is in need of a restroom break. He is aware of the company's policy that requires users to logoff their computers when not in use. However, Pat hates the inconvenience of logging out and logging back in again, so he does not log off his computer when he leaves his desk to visit the restroom.

USB Copy Scenario

Chris is an employee in your organization and is currently working on a report that requires the analysis of sensitive company data. He is extremely busy and wants to continue working on the report later that evening at home. Chris is aware of your company's policy that prohibits users from copying company data to portable media, such as USB drives, to avoid security problems. However, Chris copies several company files to his personal, unencrypted USB drive so that he can work on the report at home.

Data Leakage Scenario

Alex is an employee in the human resources department at your organization and thus has been authorized to view the salary information of all employees as part of his job functions. Recently, one of Alex's friends (who does not work for your organization) contacted Alex and asked for the salary information of all managers in your organization. The friend informed Alex that he was applying for a management position in your organization and wanted to use the information to determine what salary to ask for in case he is offered the position. Although Alex believes that providing the salary information is a violation of company policy, he looks it up and gives it to the friend.

Table A1. Scenario-Specific Items—INT, MB, and PS

Item number	Item
INT1	How likely is it that you would have done the same as Jim in that situation? (Very unlikely/Very likely)
INT2	I could see myself sharing the password as Jim did. (Strongly disagree/Strongly agree)
MB1	It is morally unacceptable to do what Jim did in that situation. (Strongly disagree/Strongly agree)
MB2	It is against my moral belief to do what Jim did in that situation. (Strongly disagree/Strongly agree)
PS1 (certainty)	What is the likelihood that Jim would be formally punished? (Very unlikely/Very likely)
PS2 (certainty)	Jim would be reprimanded at some point for sharing the password. (Strongly disagree/Strongly agree)
PS3 (severity)	If punished, how severe would Jim's punishment be? (Not severe at all/Very severe)
PS4 (severity)	Jim would receive harsh sanctions for sharing the password. (Strongly disagree/Strongly agree)
PS5 (celerity)	If punished, Jim's punishment would be immediate. (Strongly disagree/Strongly agree)
PS6 (celerity)	If punished, Jim's punishment would be timely. (Strongly disagree/Strongly agree)

Notes: These items followed the scenario, in scrambled order. The items pertain to the password-sharing scenario; item wordings were slightly modified to fit each scenario. The survey instructions told respondents to consider the scenario in the context of their own organization. INT = ISP violation intention; MB = moral belief; PS = perceived sanctions.

Table A2. Scenario-Specific Items—Moral Disengagement (MD)

Item number	MD mechanism	MD category	Item
MJ1	MJ	RC	It is alright to share a password to get work done quicker.
MJ2	MJ	RC	It is alright to share a password if it helps you do your job more efficiently.
MJ3	MJ	RC	It is alright to share a password when you are in a hurry and the work needs to get done.
EL1	EL	RC	It is not such a bad thing to share a password if the situation calls for it.
EL2	EL	RC	Password sharing is really just a reality in the workplace.
EL3	EL	RC	Sharing a password with a coworker is no big deal.
PC1	PC	RC	An employee's good job performance should compensate for occasional policy violations such as sharing a password.
PC2	PC	RC	Sharing a password is no big deal when you consider that more severe policy violations happen all of the time.
PC3	PC	RC	Compared to other security policy violations, password sharing is minor.
DR1	DR	OC	Employees cannot be blamed for sharing a password if they are overloaded with work tasks.
DR2	DR	OC	If management does not want password sharing, they should put in place better workarounds.
DR3	DR	OC	Employees cannot be blamed for sharing passwords because it is difficult to get the job done otherwise.
DFR1	DFR	OC	An employee cannot be blamed for sharing a password because many factors contribute to this action.
DFR2	DFR	OC	It is unfair to blame one employee for sharing a password when many others do the same.
DFR3	DFR	OC	It is unfair to blame one employee for sharing a password because he/she has limited responsibility for information security.
DC1	DC	OC	Sharing a password really won't hurt the organization.
DC2	DC	OC	Giving a password to a coworker if he/she needs it doesn't really do any harm.
DC3	DC	OC	It is okay to share a password because no direct damage is done to the company.
DH1	DH	DT	If feel it is okay to violate policy, such as sharing a password, because my company is so bureaucratic.
DH2	DH	DT	My organization is really not people oriented, so I don't mind violating a policy that prohibits password sharing.
DH3	DH	DT	Violating policy, such as sharing passwords, is fine because my company lacks consideration for its employees.
AB1	AB	DT	It is okay to share a password because a policy that prohibits this action is too restrictive.
AB2	AB	DT	It is okay to share a password because a policy that prohibits this action is unreasonable.
AB3	AB	DT	It is okay to share a password because a policy that prohibits this action is too strict.

Notes: These items followed the scenario and related items in Table A1, and were presented in scrambled order. The items above pertain to the password-sharing scenario—item wordings were slightly modified to fit each scenario. All items were measured using a seven-point scale with "strongly disagree" to "strongly agree" as anchors. MJ = moral justification; EL = euphemistic labeling; PC = palliative comparison; DR = displacement of responsibility; DFR = diffusion of responsibility; DC = distortion of consequences; DH = dehumanization; AB = attribution of blame; RC = reconstruing the conduct; OC = obscuring or distorting consequences; DT = devaluing the target.

Table A3. Security-Related Stress (SRS) Items

Item number	SRS dimension	Item
Dropped	Complexity	I sometimes feel pressure in my job due to information security requirements.
CX2	Complexity	I find that new employees often know more about information security than I do.
CX3	Complexity	I do not know enough about information security to comply with my organization's policies in this area.
CX4	Complexity	I often find it difficult to understand my organization's information security policies.
CX5	Complexity	It takes me awhile to understand my organization's information security policies and procedures.
CX6	Complexity	I sometimes do not have time to comply with my organization's information security policies.
OL1	Overload	I am forced by information security policies and procedures to do more work than I can handle.
OL2	Overload	My organization's information security policies and procedures hinder my very tight time schedules.
OL3	Overload	I have a higher workload due to increased information security requirements.
OL4	Overload	I am forced to change my work habits to adapt to my organization's information security requirements.
UC1	Uncertainty	There are constant changes in information security policies and procedures in my organization.
UC2	Uncertainty	There are frequent upgrades to information security procedures in my organization.
UC3	Uncertainty	There are always new information security requirements in my job.
UC4	Uncertainty	There are constant changes in security-related technologies in my organization.

Notes: These items followed the scenario-specific items, in a separate section, and were presented in scrambled order. All items were measured using a seven-point scale with "strongly disagree" to "strongly agree" as anchors. CX = SRS complexity; OL = SRS overload; UC = SRS uncertainty.

Table A4. Ethical Orientation, Social Desirability Bias, and Marker Variable Items

Item number	Item
IDEAL1	People should make certain that their actions never intentionally harm another even to a small degree.
IDEAL2	Risks to another should never be tolerated, irrespective of how small the risks might be.
IDEAL3	The existence of potential harm to others is always wrong, irrespective of the benefits gained.
IDEAL4	One should never psychologically or physically harm another person.
IDEAL5	One should not perform an action which might in any way threaten the dignity and welfare of another individual.
IDEAL6	If an action could harm an innocent other, then it should not be done.
Dropped	Deciding whether or not to perform an action by balancing the positive consequences of the act against the negative consequences is immoral.
IDEAL7	The dignity and welfare of the people should be the most important concern in any society.
Dropped	It is never necessary to sacrifice the welfare of others.
Dropped	Moral behaviors are actions that closely match the ideals of the most "perfect" action.
Dropped	There are no ethical principles that are so important that they should be a part of any code of ethics.
REL1	What is ethical in society varies from one situation to another.
Dropped	What one person considers moral may be judged to be immoral by another.
Dropped	Different types of morality cannot be compared as to "rightness."
REL2	Questions of what is ethical for everyone can never be resolved since what is moral or immoral is up to the individual.
REL3	Moral standards are simply personal rules that indicate how a person should behave and are not to be applied in making judgments of others.
REL4	Ethical considerations in interpersonal relationships are so complex that individuals should be allowed to formulate their own ethical codes.
REL5	Rigidly codifying an ethical position that prevents certain types of actions could stand in the way of better human relations.
REL6	No rule concerning lying can be formulated; whether a lie is permissible or not totally depends on the situation.
REL7	Whether a lie is judged to be moral or immoral depends upon the circumstances surrounding the action.
SDB1	I am always courteous even to people who are disagreeable.
SDB2	No matter who I'm talking to, I'm always a good listener.
SDB3	I am always willing to admit it when I make a mistake.
Dropped	I have never intensely disliked anyone.
SDB4	I would never think of letting someone else be punished for my wrongdoings.
OA1	I like outside activities better than inside activities.
OA2	I like to meet my friends at a restaurant more than at home.
OA3	I like to do athletic sports.
OA4	I exercise moderately every day.
OA5	I like to travel abroad whenever possible.

Notes: These items followed the items in Tables A1–A3, in a separate section, and were presented in scrambled order. All items were measured using a seven-point scale with "strongly disagree" to "strongly agree" as anchors. IDEAL = idealism; REL = relativism; SDB = social desirability bias; OA = outside activity.

Appendix B: Demographic Characteristics of Respondents

Survey participants (n = 539)			
Gender	Male	272	50.5
	Female	267	49.5
Age	18–24	13	2.4
	25–34	142	26.3
	35–44	129	23.9
	45–54	144	26.7
	55 and over	111	20.6
Education	High school	97	18.1
	Two-year college	102	19.0
	Bachelor's degree	214	39.9
	Master's degree	86	16.0
	Doctoral degree	21	3.9
	Other	17	3.2
Position	Senior manager	45	8.3
	Middle manager	118	21.9
	Technical	78	14.5
	Professional staff	134	24.9
	Administrative	102	18.9
	Other	62	11.5
Industry	Manufacturing	61	11.3
	Banking/finance	52	9.6
	Information technology	52	10.4
	Health care	65	12.1
	Government	63	11.7
	Utility	13	2.4
	Academic/education	62	11.5
	Wholesale or retail	60	11.1
	Other	107	19.9

	Mean	Standard deviation
Organizational tenure (years)	12.3	9.56
Computer use at work (hours/day)	7.53	3.53
Self-rated computer knowledge (1–7) scale	5.52	0.973