Journal of the Association for Information Systems

Volume 17 | Issue 1 Article 4

1-27-2016

Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess

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

Paul Benjamin Lowry
City University of Hong Kong, paul.lowry.phd@gmail.com

Jordan B. Barlow
California State University, Fullerton, jobarlow@fullerton.edu

Recommended Citation
Wall, Jeffrey D.; Lowry, Paul Benjamin; and Barlow, Jordan B. (2016) "Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess," *Journal of the Association for Information Systems*, 17(1), .
DOI: 10.17705/1jais.00420
Available at: https://aisel.aisnet.org/jais/vol17/iss1/4

Journal of the Association for Information Systems

Research Paper ISSN: 1536-9323

Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess

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

Paul Benjamin Lowry
Department of Information Systems, City University of Hong Kong, Hong Kong

Jordan B. Barlow
California State University, Fullerton, USA

Abstract:

Privacy and security concerns are pervasive because of the ease of access to information. Recurrent negative cases in the popular press attest to the failure of current privacy regulations to keep consumer and protected health information sufficiently secure in today's climate of increased IT use. One reason for such failure is that organizations violate these regulations for multiple reasons. To address this issue, we propose a theoretical model to explain the likelihood that organizations will select an externally governed privacy or security rule for violation in response to organizational strain or slack resources. Our proposed theoretical model, the selective organizational information privacy and security violations model (SOIPSVM), explains how organizational structures and processes, along with characteristics of regulatory rules, alter perceptions of risk when an organization's performance does not match its aspiration levels and, thereby, affects the likelihood of rule violations. Importantly, we contextualize SOIPSVM to organizational privacy and security violations. SOIPSVM builds on and extends the selective organizational rule violations model (SORVM), which posits that organizational rule violations are selective. SOIPSVM provides at least four contributions to the privacy and security literature that can further guide empirical research and practice. First, SOIPSVM introduces the concept of selectivity in rule violations to privacy and security research. This concept can improve privacy and security research by showing that organizational violations of privacy and security rules are dynamic and selective yet influenced by external forces. Second, SOIPSVM extends the boundaries of SORVM, which is limited to explaining the behavior of organizations under strain, such as economic hardship. We contribute to the theory of selective deviance by proposing that selectivity extends to organizations with slack resources. Third, we address ideas of non-economic risk and strain in addition to economic risk and strain. Thus, SOIPSVM explains organizational rule-violating behavior as an attempt to protect core organizational values from external entities that pressure organizations to change their values to comply with rules. Fourth, we broaden the theoretical scope of two important constructs (namely, structural secrecy and procedural emphasis) to improve the model's explanatory power. Fifth, we identify important elements of rule enforcement by drawing from the tenets of general deterrence theory. We also discuss how one can study constructs from general deterrence theory at the organizational level. To conclude, we offer recommendations for the structuring of organizations and external regulations to decrease organizational rule violations, which often lead to the abuse of consumer information.

Keywords: Selective Organizational Information Privacy And Security Violations Model (SOIPSVM), Privacy, Security, Theory Building, Organizational Privacy, Organizational Security, Rule Violations, Policy Violations, Information Abuse, SOIPSVM, PCI DSS, HIPAA, Selective Organizational Rule Violations Model (SORVM).

Paul Pavlou was the accepting senior editor. This paper was submitted on December 30, 2013 and went through three revisions.

1 Introduction

Information privacy and security are becoming increasingly important in an ever more connected and information-intensive world. As a result, information privacy and security laws have become prevalent in many areas of society. This trend began with the Fair Credit Reporting Act in 1971; other privacy laws, such as the Family Educational Rights and Privacy Act, soon followed. With the advent of the Internet and the associated ease of distributing information, privacy and security laws relating to information systems (IS) also emerged. Examples include the Federal Information Security Management Act and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Even for-profit industries have established externally governed rules for privacy and security, such as the Payment Card Industry Digital Security Standard (PCI DSS).

In this paper, externally governed privacy and security rules refer to laws, directives, policies, and standards pertaining to privacy and security that are developed by agencies or collectives (governmental or industrial) external to the organizations subject to the rules. Moreover, the external agencies or collectives enforce the privacy and security rules through monitoring and/or sanctions and fines.

Despite the existence of these externally governed rules, organizations continue to violate IT privacy and security rules by misusing protected data purposefully or by failing to protect it adequately (e.g., Anton, He, & Baumer, 2004; Culnan & Williams, 2009). Organizational violations of externally governed privacy and security rules can be extremely damaging (Acquisti, Friedman, & Telang, 2006). For example, Citigroup's violations of the Sarbanes–Oxley Act (SOX) resulted in securities fraud and cost investors more than USD$700 million (Calabresi, 2011). Individuals lodge thousands of complaints annually against organizations for their misusing protected healthcare information in violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (EMS Insider, 2008). Credit card fraud resulting from PCI DSS violations affects millions of consumers each year (Shaw, 2010).

In response to these issues, a growing body of behavioral security research has looked at ways to help individual employees better protect the security and privacy of their organizations. Some have looked at ethical and moral issues that inspire bad employee behavior (Culnan & Williams, 2009; Lowry, Posey, Roberts, & Bennett, 2014). Some have looked at issues of perceived fairness or loss of freedom that can cause employees to act out negatively toward security and privacy policies (Lowry & Moody, 2015; Lowry, Posey, Bennett, & Roberts, 2015). Some have considered rational choice and cost/benefit decisions in security compliance (Bulgurcu, Cavusoglu, & Benbasat, 2010; Hu, Xu, Dinev, & Ling, 2011a). Low self-control and neutralization are also important individual-level considerations in the literature (Barlow, Warkentin, Ormond, & Dennis, 2013; Hu et al., 2011a; Siponen & Vance, 2010). Some have adapted deterrence theory from criminology research to see if one can threaten employees into compliance (D'Arcy & Herath, 2011). Researchers have also looked at non-invasive ways that one can make employees experience higher levels of accountability for their organizational security and privacy behaviors (Vance, Lowry, & Eggett, 2013, 2015). Some have considered using fear appeals to motivate employees to protective themselves and organizations from security and privacy breaches (Boss, Galletta, Lowry, Moody, & Polak, 2015; Johnston & Warkentin, 2010). Researchers have also carefully considered the key protective motivation and extra-role behaviors employees should follow for improved security outcomes (Hsu, Shih, Hung, & Lowry, 2015; Posey, Roberts, Lowry, Bennett, & Courtney, 2013).

The downside of this body of research is that it focuses virtually only on employees themselves and not the organizational environment and organizational-level decisions. Consequently, the related theories and empirical evidence are on the individual level, not the organizational level. Despite the importance of organizational privacy and security, actual organization-level IS privacy and security research is in a nascent state, which has led to calls for more organization-level research (Belanger & Crossler, 2011; Crossler et al., 2013; Pavlou, 2011; Smith, Dinev, & Xu, 2011). In particular, we know little about what causes organizations to choose to engage in serious privacy and security violations of stakeholder rights. In a separate stream of organizational research, Lehman & Ramanujam (2009) have proposed a theoretical model, which we refer to as the selective organizational rule violations model (SORVM), that posits that organizational rule violations are selective. That is, violations do not necessarily result solely from bad organizational processes or bad rules. Rather, combinations of organizational and rule characteristics lead organizations to selectively decide to violate certain rules (Lehman & Ramanujam, 2009). Although researchers have not applied SORVM to studies in an organizational privacy and security context, it provides an important theoretical foundation that can lead to deeper conceptualization in our context. We need a new organizational-level theory in the information privacy and security context because previous

research has focused on organizational privacy and security behavior solely in terms of organizational characteristics (e.g., Greenaway & Chan, 2005) or rule characteristics (e.g., Hooper & Vos, 2009; Walczuch & Steeghs, 2001) in isolation. Moreover, SORVM is not contextualized to privacy and security, whereas the best kinds of theories that are more likely to be tested and to contribute to practice are highly contextualized (e.g., Eisenhardt, 1989; Whetten, Felin, & King, 2009; Whetten, 2009), as Boss et al. (2015) recently demonstrated in a security context.

We call our new, highly contextualized organizational-level model the selective organizational information privacy and security violations model (SOIPSVM). We designed SOIPSVM to answer the following research questions:

RQ1: Does the idea of "selective" rule violations apply in explaining organizational-level violations of privacy and security rules?"

RQ2: A key conceptual limitation of SORVM is that it is limited to explaining the behavior of organizations under strain, such as economic hardship. Yet, many thriving organizations have intentionally violated the privacy or security of their stakeholders. Thus, does the concept of selectivity also extend to organizations with slack resources?

RQ3: Another conceptual limitation of SORVM is that its "strain" concept is based on economic factors. Yet, in a privacy or security context, organizational strain could occur for many non-economic reasons, such as regulatory pressure and consumer expectations. Thus, can we extend this conceptual foundation to account for non-economic sources of strain?

RQ4: Can we apply privacy and security concepts from individual-level research, such as deterrence theory and its related constructs, at the organizational level to help explain organizational violations of privacy and security rules?

To explain SOIPSVM and answer these research questions, we proceed as follows. In Section 2, we review of the existing organization-level research relating to organizational rule, policy, and ethics violations in the context of information privacy and security. In Section 3, we outline key theoretical foundations and assumptions and demonstrate how organization-level privacy and security violations fit in the assumptions and constraints of SORVM. In Section 4, we discuss the need to extend and contextualize SORVM. In Section 5, building on SORVM, we propose SOIPSVM and carefully contextualize it and extend it to address our research questions. We include examples relating to HIPAA, PCI DSS, and SOX to demonstrate our model's usefulness in the information security and privacy domain. We also discuss the applicability of our model to a well-known case of organizational rule violations, the TJX Companies, which resulted in security breaches that SOIPVSM explains well. In Section 6, we explain ways in which future research can operationalize and test SOIPVSM aside from case studies. Finally, in Section 7, we conclude the paper.

2 Organizational Privacy and Security Violations

Researchers have attempted to explain organizational rule violations from a variety of perspectives. Research on corruption in organizations has shown that organizational violations are a serious issue (Acquisti et al., 2006; Ashforth & Anand, 2003; Pinto, Leana, & Pil, 2008), but little research has investigated the processes that lead to these violations (Vaughan, 1999; Vaughan, 2002). Some studies have focused on organizational processes as antecedents to rule violations (Ashforth, Gioia, Robinson, & Treviño, 2008; Brief, Buttram, & Dukerich, 2000), whereas others have noted that the rules' characteristics themselves are key drivers of violations (Beck & Kieser, 2003; Lange, 2008; March, Schulz, & Zhou, 2000; Zhou, 1993). Lehman and Ramanujam (2009) bridge these research streams by creating a theoretical model (SORVM) that incorporates both organizational context and rule characteristics as predictors of rule violations resulting from perceptions of risk.

Organizational rule violations include all illegal or unethical actions that an organization commits; however, we deal with only a subset of these violations: privacy and security rule violations. In their literature reviews, Belanger and Crossler (2011) and Smith et al. (2011) offer an in-depth examination of information privacy and security literature at all levels of analysis. From the papers these studies review, we selected and reviewed organization-level journal papers closely related to our focus: compliance and non-compliance with externally governed rules. We categorized the papers into those that examined internal rules (e.g., company policies) and those that examined externally governed rules (e.g., laws). We also categorized the papers by privacy context; most papers fell into the categories of organization-to-consumer interactions or organization-to-employee interactions. Some

papers fit into multiple categories. Table 1 categorizes the papers by policy type (i.e., external or internal policies) and by privacy context (i.e., consumer- or employee-centric).

Table 1. Organization-level Privacy and Security Compliance Studies by Policy Type and Privacy Context

Policy type	Consumer-centric privacy	Employee-centric privacy
Internal policy/ethical perspective	Agranoff (1991), Bennasi (1999), Culnan (2000), Culnan & Bies (2003), Desai, Richards, & Desai (2003), Greenaway & Chan (2005), Henderson & Snyder (1999), Jafar & Abdullat (2009), Milne, Culnan, & Greene (2006), Miyazaki & Fernandez (2000), Miyazaki & Krishnamurthy (2002), Moores & Dhillon (2003), Peslak (2005, 2006), Pollach (2007), Ryker, Lafleur, McManis, & Cox (2002), Smith (1993), Storey, Kane, & Schwaig (2009)	Ariss (2002), Greco (2001), Schein (1977), Sewell & Barker (2001), Sipior, Ward, & Rainone (1998)
External policy/legal perspective	Agranoff (1991), Culnan & Bies (2003), Dhillon & Moores (2001), Greenaway & Chan (2005), Hooper & Vos (2009), Milne & Culnan (2002), Schwaig, Kane, & Storey (2006), Walczuch, Singh, & Palmer (1995), Walczuch & Steeghs (2001)	Ariss (2002), Friedman & Reed (2007), Greco (2001), Nord & McCubbins (2006), Walczuch & Steeghs (2001)

Most privacy and security studies, whether consumer- or employee-centric, focus primarily on internal, not external, policy compliance. Studies focusing on externally governed privacy and security rules, whether consumer- or employee-centric, are primarily exploratory and descriptive in nature probably because data collection is difficult in this research area (Crossler et al., 2013; Dhillon & Moores, 2001; Milne & Culnan, 2002; Nord & McCubbins, 2006; Walczuch & Steeghs, 2001). Much security and privacy research uses surveys or hypothetical scenarios (e.g., D'Arcy, Hovav, & Galletta, 2009; Siponen & Vance, 2010), both of which may be difficult to apply to an organization-level analysis of external policies.

Other research (e.g., Hooper & Vos, 2009; Milne & Culnan, 2002; Schwaig et al., 2006) explores the extent to which businesses obey privacy laws. Dhillon and Moores (2001) use a subjective analysis of survey panels to identify individuals' major concerns regarding organizations' adherence to privacy standards. Walczuchand and Steeghs (2001) use interviews to explore the possible negative and positive effects of adhering to data-protection legislation in the European Union.

Culnan and Bies (2003), Walczuch et al. (1995), and Greenaway and Chan (2005) have conducted the few theoretically grounded studies in this area. Culnan and Bies examine consumer-organization privacy interaction from the perspective of justice theories. They suggest that organizations can implement fair information practices in three ways: through government regulation, self-regulation, and technological solutions. Such information practices should align with consumer perceptions of what constitutes the just use of consumer information. Walczuch et al. develop a conceptual model to explain the development of laws relating to international data flows. Their model suggests that culture, in the form of values and ideologies, affects economic considerations and the public policy-creation process. They also argue that public policy formulation processes affect the likelihood that regulators will develop data-flow legislation.

Greenaway and Chan (2005) discuss theories that explain information privacy behaviors including, but not limited to, compliance with laws and standards. They propose two approaches (the institutional approach, a perspective that examines organizational behavior in the context of social, political, and cultural environments, and the resource-based view, a perspective that emphasizes economic and competitive advantage as a driver of organizational behavior) as theories that explain information privacy behavior. However, they focus only on organizations and not on the characteristics of laws and standards in explaining privacy violations theoretically. Thus, they fail to capture adequately the relationship between regulators and organizations.

Despite these papers' theoretical contributions, they fail to offer a strong theoretical foundation that can explain organizations' violations of externally governed information privacy and rules by examining both organizational context and rule characteristics. Further, these models mostly fail to capture the selective and dynamic nature of decision processes that affect organizational violations. SOIPSVM represents our attempt to fill this gap. The lack of a strong theoretical foundation in organizational privacy and security violations limits our understanding of what causes some organizations to follow rules and others to violate them. Without understanding why organizations choose to violate or follow rules, it is difficult to devise

appropriate controls to minimize non-compliance. Thus, we propose a theoretical foundation that can assist researchers in understanding why organizations violate privacy and security rules.

3 Historical and Foundational Theory

We base our model on the assumptions and propositions expounded in SORVM, which explains why organizations selectively violate some rules while complying with others. Our adaptation of SORVM better describes violations of externally governed IT privacy and security rules, particularly those prescribed by HIPAA, PCI DSS, and SOX.

3.1 An Overview of SORVM: Explaining Selectivity in Rule Violations

SORVM (see Figure 1) posits that organizations violate rules on a selective basis (Lehman & Ramanujam, 2009). SORVM is founded primarily on institutional logics (Pfeffer & Salancik, 1978), organizational decision theory (Cyert & March, 1963), and the theory of organizational response to strain (e.g., performance issues) (Merton, 1938). SORVM accounts for agency by relying on theories of organizational decision making. In SORVM, an organization's perceptions of risk and focus of attention—two important factors influencing organizational decision making—mediate the relationship between contextual conditions and rule characteristics and the likelihood of a rule violation. In Sections 3.2 to 3.2.4, we explain the model's key assumptions and then describe the constructs and relationships in detail.

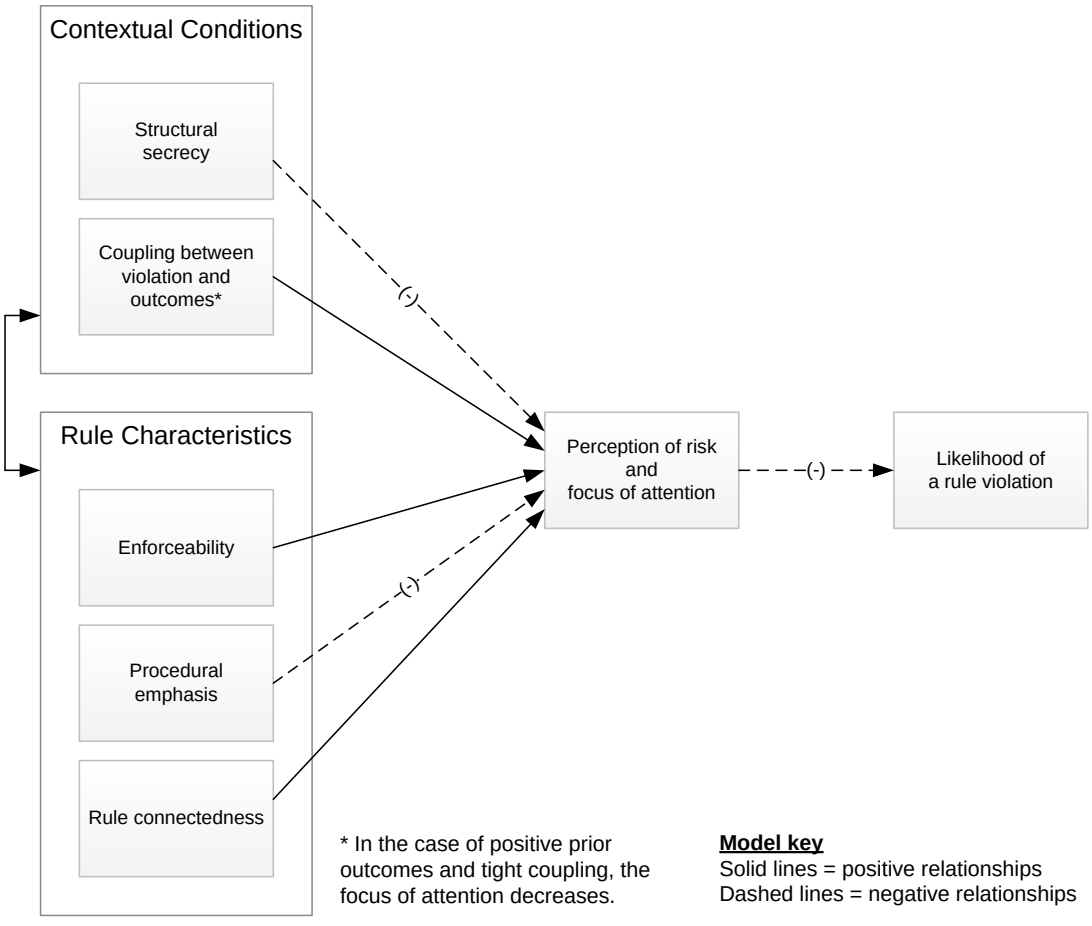

Figure 1. Selective Organizational Rule Violations Model (Lehman & Ramanujam, 2009)

3.2 Key assumptions of SORVM

Table 2 categorizes SORVM's assumptions and constraints into those dealing with rules, those dealing with organizations, and those dealing with violations. The assumptions dealing with rules limit the model's direct extension to other forms of social guidance or restraint, such as norms or ungoverned standards. First,

SORVM views rules as constraints on organizational members and not as moral principles that define social roles. Second, SORVM focuses on external, formalized rules, such as laws. Third, SORVM is limited to rules that are low in ambiguity, which means that organizations will have similar interpretations of the rules (Lehman & Ramanujam, 2009).

Table 2. Assumptions of SORVM (Lehman & Ramanujam, 2009)

Category of assumptions	Specific assumptions of the model
Rules	Rules are constraints on organizational action and not moral principles (p. 645).
	Rules must be external and formal like laws (p. 644).
	Rules must be low in ambiguity (p. 644).
Organizations	Groups with access to critical resources predominantly determine organizational actions (p. 646).
	Theoretical scope includes only organizations vulnerable to committing violations, such as those experiencing organizational strain through performance downfalls or stiff competition (p. 646).
Rule violations	Rule violations do not include individuals' violations for personal gain or sabotage (p. 644).
	Rule violations result from satisficing solutions devised to address limits to organizational attention that present themselves during the search for solutions to performance issues (p. 646).
	Rule violations focus on critical organizational resources and the interests of powerful organizational coalitions (p. 647).

Next, SORVM holds two key assumptions about organizations. First, organizational members form coalitions that develop goals and perceptions of organizational situations and circumstances that may conflict with other coalitions (March & Simon, 1958). When conflict occurs between coalitions, the coalition(s) with access to more critical organizational resources exert greater influence over organizational actions (Pfeffer & Salancik, 1978). Second, some organizations are more vulnerable to committing violations than others are. Strain theory (Merton, 1938) suggests that entities may seek to achieve their goals through deviant or non-routine behaviors when they are unable to do so through legitimate means. Organizations that experience strain, such as performance downfalls, may be more vulnerable to committing rule violations (Lehman & Ramanujam, 2009).

The remaining three SORVM assumptions limit which type of violations the model can explain. First, SORVM considers only violations made in conjunction with sanctioned organizational decisions. Because SORVM is an organization-level theory, individual-level deviance, such as unsanctioned sabotage behavior, lies outside its scope. Second, when organizations look for solutions to performance issues or ways to use slack resources, organizational attention is limited (March & Simon, 1958), which, in turn, limits the number of decision alternatives (Ocasio, 2002). Third, because organizational attention is limited, organizations will focus their attention mainly on rules affecting critical resources or the interests of powerful organizational coalitions (Lehman & Ramanujam, 2009), which occurs because organizations seeking to relieve performance downfalls frame solutions in terms of regaining and maintaining critical resources (Pfeffer, 1992).

3.2.1 Likelihood of Rule Violation

SORVM's ultimate objective is to predict the likelihood that an organization will violate a rule. The *likelihood of a rule violation* refers to the degree to which systemic factors in the organization and regulatory environment prompt it to violate some rule (Lehman & Ramanujam, 2009).

3.2.2 Mediating Constructs: Perceptions of Risk and Focus of Attention

In SORVM, the mediating variable perceptions of risk refers to the extent to which an organization will perceive a rule violation as having negative outcomes that are certain, severe, and uncontrollable (March & Shapira, 1987). Perceptions of risk have a negative relationship with the likelihood that an organization will violate a rule. Importantly, SORVM only conceptualizes perceptions of risk as economic in nature. The perceived risk of implementing each alternative filters the solutions to performance downfalls (Shapira, 1997; Slovic, 2000). When an organization perceives a solution as more risky, the likelihood of a rule violation will decrease, and the converse holds for solutions perceived as less risky (Lehman & Ramanujam, 2009).

The other mediating variable, focus of attention, refers to the issues and possible actions on which decision makers in an organization emphasize. Focus of attention is important because "decision-makers will be selective in the issues and [solutions] they attend to at any one time and…what decision-makers do depends on what issues and [solutions] they focus their attention on" (Ocasio, 1997, p. 189). Organizational attention, overall, is limited (March & Simon, 1958), which, in turn, limits the number of decision alternatives when organizations look for remedies for performance issues (Ocasio, 2002). Although not all alternative solutions will lead to rule violations, many decision alternatives can lead to violations (Alexander & Cohen, 1996; Harris & Bromiley, 2007).

Further, because organizational attention on any issue is limited, organizations will focus their attention mainly on rules affecting critical resources or the interests of powerful organizational coalitions (Lehman & Ramanujam, 2009), which occurs because organizations seeking to relieve performance downfalls frame solutions in terms of regaining and maintaining critical resources (Pfeffer, 1992).

3.2.3 Contextual Conditions: Structural Secrecy and Violation Coupling

The two major elements of contextual considerations are structural secrecy and coupling between violations and outcomes.

SORVM proposes that structural secrecy decreases risk perceptions. Structural secrecy refers to "the way that patterns of information, organizational structures, processes, and transactions, and the structure of regulatory relations systematically undermine the attempt to know and interpret situations in organizations" (Vaughan, 1996, p. 238). Structural secrecy influences internal decision making processes, which influence the likelihood that decision makers will engage in deviant behavior in pursuing organizational goals (Lehman & Ramanujam, 2009). Decreasing secrecy makes hiding rule violations more difficult and costly (Lehman & Ramanujam, 2009). Thus, structural secrecy influences the degree to which external pressures sway decision makers' choices. When secrecy is high, isolating rule-related power and knowledge helps to minimize potential conflicts related to violations (Vaughan, 1996), which decreases perceptions of risk related to rule violations (Lehman & Ramanujam, 2009).

Violation coupling refers to "the perceived likelihood that…violations will lead to known outcomes—either positive, such as a performance improvement, or negative, such as regulatory penalties" (Lehman & Ramanujam, 2009, p. 648). When coupling is tight, the connection between violations and their associated outcomes is easily discernible, and organizational members perceive the outcome of a violation as predictable (Lehman & Ramanujam, 2009). When coupling is tight and organizational members perceive prior violation outcomes to be positive, organizational members feel a sense of control over the potential consequences (Shapira, 1997). When violators go unpunished, the consistent benefits of violation lead to a sense of control over outcomes. Therefore, organizational members are less likely to perceive violations tightly coupled to positive outcomes as risky and will more likely repeat them (Lehman & Ramanujam, 2009). For example, an organization that gains financially from violating a rule and that does not receive a penalty for it will associate the rule violation with positive outcomes and, thereby, decreasing risk perceptions. Violations tightly coupled to negative outcomes (e.g., fines and sanctions, tarnished corporate image), however, direct attention to the negative consequences associated with a particular behavior. The perceived certainty of the negative consequences increases perceptions of risk by decreasing organizational members' sense of control over the organizational situations (Lehman & Ramanujam, 2009).

3.2.4 Rule Characteristics: Enforceability, Procedural Emphasis, and Rule Connectedness

The three major elements of rule characteristics are enforceability, procedural emphasis, and rule connectedness.

SORVM proposes that the enforceability of a privacy or security rule is a rule characteristic that affects the likelihood that an organization will violate the rule by increasing perceived risk. Enforceability is the extent to which organizations view regulatory agencies as able and likely to monitor compliance with a rule and to seek justice for violations (Fuller, Edelman, & Matusik, 2000). In this way, enforceability is similar to coercive pressures in neoinstitutionalism.

Procedural emphasis refers to whether a rule's content emphasizes procedures over outcomes (Lange, 2008). SORVM predicts that procedural emphasis decreases perceptions of risk for several key reasons. When procedural emphasis is high, the desired outcomes of a rule are ambiguous, which suggests low goal clarity. When procedural emphasis is low, a rule is unambiguous and desired outcomes are clearly defined (Edelman, 1992); that is, goal clarity is high. Organizational interpretations of a rule in situations where the

rule's goal is unclear can lead to a routinized interpretation of the rule even in unambiguous situations (Lehman & Ramanujam, 2009). The pursuit of critical organizational resources tend to guide interpretations of rules (Lehman & Ramanujam, 2009). Power struggles over the interpretations of a rule create emerging meaning about how organizational members are to perceive the rule (e.g., important or unimportant) and what efforts, if any, organizational members should take to conform to the rule (Pfeffer, 1992). Powerful organizational members then legitimize the emerging meaning in support of their particular interpretations (Johnson, Dowd, & Ridgeway, 2006), and these interpretations become stabilized methods for maintaining and acquiring critical resources (Lehman & Ramanujam, 2009). As organizations routinize these interpretations of rules, organizational members view them as predictable and controllable (March, 1997). Hence, the routinized interpretations cause perceptions of risk to decrease even in unambiguous situations (Lehman & Ramanujam, 2009).

Rule connectedness refers to the amount of interdependence or the number of functional links a rule has with other rules (March et al., 2000). When connectedness is high, a rule is interdependent on many other rules—often rules in the same law. However, when connectedness is low, a rule is dependent on few or no other rules (Lehman & Ramanujam, 2009). Rule connectedness increases perceived risk in three ways. First, coordination costs increase when rules are interdependent (Feldman & Pentland, 2003). Second, when multiple regulators exist or the rule system is complex, organizational members may feel less control (Lehman & Ramanujam, 2009), which increases the likelihood that members will perceive that regulators will detect a rule violation and levy sanctions against the organization (March & Shapira, 1987). The increase in coordination costs and in the likelihood of detection increases perceptions of risk associated with violating a rule. Finally, when rules are highly connected and, consequently, overlap, a violation of one rule often leads to or includes violations of connected rules; organizations will perceive violating multiple rules as having higher risk compared to violating only one rule because the former leads to an increased likelihood of being caught (Lehman & Ramanujam, 2009). Thus, rule connectedness influences the degree to which external pressures influence decision makers.

4 Need for Extending and Contextualizing SORVM

4.1 Why We Need SOIPVSM for Organizational Privacy and Security Violations

Although SORVM is useful in predicting organizational violations, we need an extended model in the security and privacy context for at least three reasons. First, in practice, there are a large number of organizational privacy and security violations; however, little organizational theory or data (empirical or case) exist to explain, predict, and address such violations (Belanger & Crossler, 2011; Crossler et al., 2013; Pavlou, 2011; Smith et al., 2011). Individual-level violations have a plethora of theory, and yet some of the most extreme, damaging cases are on an organizational level.

Second, as noted, the best kinds of theories, which have a strong impact on research and practice, are highly contextualized theories, not general theories (e.g., Eisenhardt, 1989; Whetten et al., 2009; Whetten, 2009), which Boss et al. (2015) shows. We need SOIPVSM because organizational privacy and security violations are wreaking havoc on practice in a way that SORVM does not fully address. There are unique considerations, which other kinds of violations may not reflect, when organizations choose to violate security or privacy standards. For example, practice has traditionally treated security and privacy issues as "IT" issues and not management issues; thus, organizational decisions related to these are often treated as a "black box", unbeknownst to managers who often do not know how important these issues are until it is too late. This treatment has resulted in a checklist culture that simplifies information privacy and security to a list of menial tasks (Dhillon & Backhouse, 2001). As a result, managers frequently fall prey to unwittingly making organizational decisions that can increase the likelihood that their organization will violate privacy rules. SOIPSVM draws management attention to organizational conditions and rule characteristics that may influence rule-related decisions. By understanding how organizational conditions influence their decisions, managers can restructure the organizational environment to increase the likelihood that their organization will make legal and ethical decisions regarding privacy. Further, cultural and society perceptions and laws about privacy and security violations have changed over time, often in response to major current events (e.g., Wikileaks, revelations on the NSA's global privacy violations, the Target data breach). The technology considerations themselves are increasingly advanced and arcane. Hence, it is more difficult for organizational members to understand and keep abreast of the underlying technological, management, and legal considerations than in other more stable areas such as torts, contracts, accounting regulations, and

best human resource practices. SOIPSVM draws attention to the importance of clarity in rule development in the privacy and security context.

There is a need in both theory and practice to understand how organizational characteristics and external forces work together to influence organizations' privacy and security behaviors. SOIPSVM, as an extension of SORVM, offers a balance between deterministic approaches that focus on external influencers and organizational approaches that focus on internal, organizational structures.

Finally, some of the constructs in SORVM narrowly focus on a specific characteristic of a larger concept. SOIPSVM broadens the theoretical lens of these constructs in SORVM to the larger concept to improve the explanatory power of the model.

4.2 Using Research on Strain Theory to Extend Limitations of SORVM's Assumptions and Propositions

Following strain theory, we suggest that an aspiration level—an expected level of future performance or achievement—guides organizational actions (Cyert & March, 1963). Early work on aspiration levels suggests a single reference point for an organization's expected level of performance (e.g., March & Shapira, 1987, 1992). SORVM is grounded in this early research. More recent research, however, suggests that performance relative to aspiration levels may be more complex (Hu, Blettner, & Bettis, 2011b).

Figure 2 depicts the differing risk preferences in relation to organizational performance. SOIPSVM extends SORVM by adopting the more recent and more complex conceptualization of aspiration levels. SOIPSVM, therefore, is more extensible in its coverage of organizations because it encompasses organizations with different levels of performance.

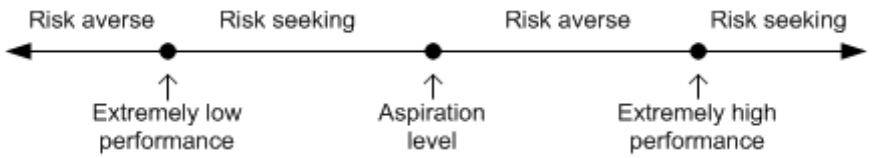

Figure 2. Organizational Risk Preferences Based on Performance Level (from (Hu et al., 2011b)

This concept allows us to extend SORVM in two key ways. First, we can expand the assumption of SORVM in terms of its application to organizations under strain to include organizations with slack resources. Second, we discuss a new moderator proposition of SOIPSVM—relative firm performance—that SORVM does not explicitly depict. We discuss these contributions in Section 5.

4.3 Necessity of Extending the Model to Include Non-economic Risk and Strain

In addition to economic strain (i.e., organizational performance), SOIPSVM considers non-economic forms of strain that influence the likelihood that an organization will violate rules. Strain theory suggests that individuals and groups unable to attain their desired goals, whether economic or non-economic, through legitimate means will be more likely to adopt deviant means to do so (Merton, 1938). Non-economic strain may result from a conflict between privacy and security rules and core organizational values. When rules conflict with core organizational values, the resulting strain may lead organizations to violate the rules to maintain their core values even when perceptions of risk are high. Present-day organizations face multiple and competing pressures; consequently, they often select which pressures to succumb to (Kostova, Roth, & Dacin, 2009). Thus, organizations may choose to violate rules rather than their core values. When core values conflict with rules, an organization's perceptions of risk may not weigh as heavily in the decision of whether to violate privacy and security rules because the risk of violating core values will exert greater influence over organizational decisions.

HIPAA rules provide a clear example of how non-economic strain influences rule-violating behavior. Doctors and nurses perceive that HIPAA rules negatively influence the quality and efficiency of patient care (Rivard, Lapointe, & Kappos, 2011), and so they may decide to violate HIPAA rules when they feel the rules conflict with patient care even if perceptions of risk are high (Lo, Dornbrand, & Dubler, 2005).

5 Proposing the Extended Theoretical Model, SOIPSVM

SOIPSVM (see Figure 3) explains violations of various organizational IS-related privacy and security rules. SOIPSVM has the potential to explain differences in compliance between rules falling under the same law. SOIPSVM can also inform the structuring of organizational and regulatory environments and the creation of privacy and security rules.

SOIPSVM is founded on SORVM's underlying theories; thus, we draw from institutional logics, theories of organizational decision making, and strain theory. In addition, by contextualizing SORVM to the privacy and security domain, we draw from theories of criminal enforcement (e.g., D'Arcy et al., 2009; Hu et al., 2011a; Siponen & Vance, 2010; Straub, 1990) and of organizational structure and information flows (Ghoshal, Korine, & Szulanski, 1994; Tsai, 2002). Moreover, we draw from research on slack resources to extend the theoretical boundaries of SORVM.

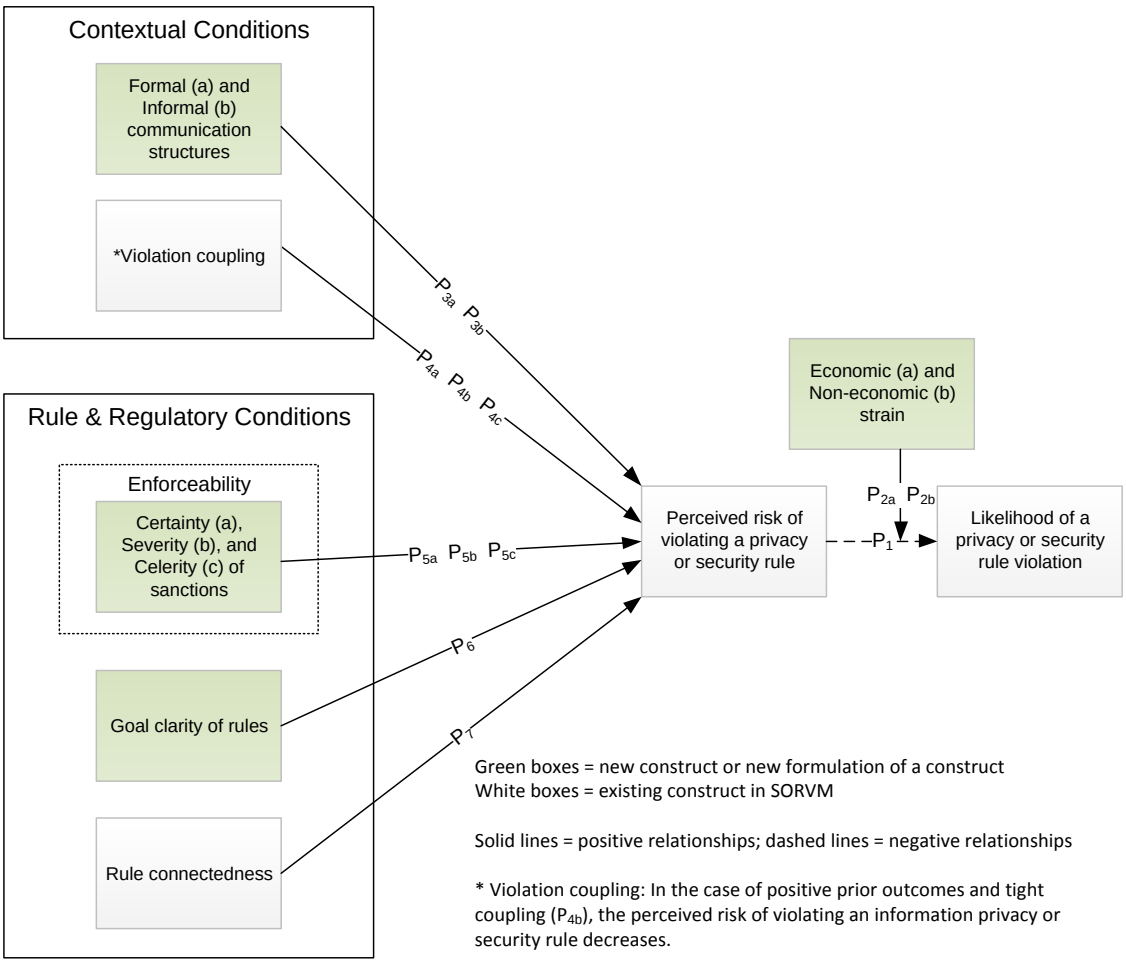

Figure 3. The Selective Organizational Information Privacy and Security Violations Model

Against this theoretical background, in Section 5.1, we explain the key elements and the basic assumptions of SOIPSVM that we retained from SORVM and those that we altered. In Sections 5.2 to 5.7, we offer propositions that contextualize and extend SORVM to the IS organizational rules and violations context. We also examine the generalizability of SOIPSVM by considering how well each proposition fits with research on HIPAA, PCI DSS, and SOX in these sections. For readers not familiar with these rules, Appendix A provides more information on all three.

5.1 Key Assumptions of SOIPVSM

At a general level, SOIPSVM adopts SORVM's key assumptions. However, we further explain and adapt these assumptions in SOIPVSM both to contextualize the theory for security and privacy rules and to refine the original theory. Table 3 lists SOIPSVM's extended and contextualized assumptions.

Table 3. Results of Discriminant Validity

Category of assumptions	Specific assumptions of the model
Rules	Rules are constraints on organizational action and not moral principles.
	Rules must be external and formal like laws.
	Rules must be low in ambiguity.
Organizations	Groups with access to critical resources predominantly determine organizational actions.
	Theoretical scope includes only organizations vulnerable to committing violations, such as those experiencing organizational strain through performance downfalls or organizations with slack resources.
Rule violations	Rule violations do not include individuals' violations for personal gain or sabotage.
	Rule violations result from satisficing solutions devised to address limits to organizational attention that present themselves during the search for solutions to performance issues. This assumption helps explain relationships between contextual conditions/rules characteristics and perceptions of risk.
	Rule violations focus on critical organizational resources and the interests of powerful organizational coalitions. This assumption helps explain relationships between contextual conditions/rules characteristics and perceptions of risk.

First, the assumptions about the types of rules considered by the model are identical in SORVM and SOIPSVM.

Furthermore, we retained the first assumption about organizations in SOIPSVM; that is, that the coalition(s) with access to more critical organizational resources exerts greater influence over organizational actions (Pfeffer & Salancik, 1978).

However, SOIPSVM extends the second assumption pertaining to organizational strain. As in SORVM, SOIPSVM assumes that some organizations are more vulnerable to committing violations than others. SORVM suggests that organizations are more likely to commit rule violations when they perform below aspiration levels. However, research on aspiration levels and risk perceptions suggests that organizations with slack resources may also engage in risky behavior (Hu et al., 2011b). Thus, SOIPSVM extends SORVM's theoretical boundaries to include organizations with slack resources in addition to organizations under financial strain. This assumption is pivotal when we describe a moderator proposition in SOIPSVM between risk perceptions and the likelihood of rule violations in Section 5.3.

SOIPSVM's remaining assumptions comprise those that constrain which type of violations the model can explain. First, as with SORVM, SOIPSVM considers only violations committed in conjunction with sanctioned organizational decisions. Individual-level deviance lies outside its scope. For example, we consider SOX regulations that hold an organization's management accountable for actions taken on behalf of the organization.

Second, SOIPSVM also assumes that, when organizations look for solutions to performance issues or ways to use slack resources, organizational attention as a whole is limited (March & Simon, 1958), which limits the number of decision alternatives (Ocasio, 2002). Although not all alternative solutions will lead to rule violations, studies show that many decision alternatives do lead to violations (Alexander & Cohen, 1996; Harris & Bromiley, 2007). Although SORVM uses this assumption to propose focus of attention as a mediating variable, SOIPSVM actually uses this concept in explaining the relationships between contextual conditions/rule characteristics and perceptions of risk.

Third, SOIPSVM continues to assume that, since organizational attention is limited, they will focus their attention primarily on rules affecting critical resources or the interests of powerful organizational coalitions (Lehman & Ramanujam, 2009). Again, this assumption drives and helps explain many of SOIPSVM's unique propositions.

5.2 Likelihood of Rule Violation

SOIPSVM contextualizes the dependent construct to focus only on the likelihood that an organization will violate security or privacy rules. The likelihood that an organization will violate security or privacy rules refers to the degree to which systemic factors in an organization and regulatory environment may prompt an organization to violate an externally governed rule established to protect the privacy and security of confidential information. We examine the generalizability of SOIPSVM by considering how well each proposition fits with research on HIPAA, PCI DSS, and SOX.

5.3 Mediating Constructs Applied to SOIPSVM

5.3.1 Perceptions of Risk Applied to SOIPVSM

Like SORVM, SOIPSVM posits that increases in an organization's perceived risk of violating an externally governed privacy or security rule will decrease the likelihood that the organization will violate the rule. SORVM conceptualizes perceptions of risk as economic in nature. However, non-economic and economic risks influence organizational decisions (Dinev & Hart, 2006). SOIPVSM extends the boundary conditions of this SORVM proposition by highlighting the influence of both non-economic and economic risk perceptions on rule violations. Negative outcomes can range from potential financial loss and decreased employee morale to the tarnishing of an organization's reputation, threats to core organizational values, and so on. When decision makers view a rule violation as risky, they will more likely not violate it due to their fearing negative outcomes from doing so (e.g., uncontrollable consequences deriving from the regulatory environment) (Lehman & Ramanujam, 2009).

Many conceptualizations of risk in the IS literature are economic in nature; that is, they define risk as the potential for economic or financial loss (e.g., Jarvenpaa, Tractinsky, & Vitale, 2000; Pavlou, 2003; Pavlou & Geffen, 2004). Similarly, SORVM is grounded in economic forms of risk (Lehman & Ramanujam, 2009). However, Dinev and Hart (2006) show that, in addition to possible financial loss, one can conceptualize risk in ways that may be more relevant to environmental factors. Our concept of perceptions of risk includes but is not limited to economic conceptualizations. Thus, we define perceptions of risk as decision makers' fear that violating an externally governed rule may have uncontrollable and negative consequences for their organization.

In an organizational privacy and security context, an organization introduces non-economic risk when it places little importance on the value of privacy and security. Organizations adopt privacy and security values to guide organizational behavior (Dhillon & Torkzadeh, 2006). However, not all organizations adopt strong privacy and security values. Many organizations simply develop security checklists and ignore deeper security values (Dhillon & Backhouse, 2001). Symbolic compliance, such as using checklists, helps to decrease risk perceptions (Lehman & Ramanujam, 2009) but not in a useful manner. Symbolic compliance refers to documenting or demonstrating actions that an organization takes to appease external entities regarding rule compliance when actual organizational behavior may be contrary to a rule's larger purpose. Symbolic compliance, such as checklists, act as a façade of compliance. Conversely, an organization with strong privacy and security values will be more likely to view privacy and security rule violations as a risk to the organization's core values. Thus, organizations with strong privacy and security values will perceive greater risk in violating a privacy and security rule than organizations with weak privacy and security values.

Perceptions of risk "vary across organizations, depending on their histories, structures, and cultures" (Lehman & Ramanujam, 2009, p. 646). Organizations will select solutions to organizational strain or slack resources based on perceived risk (Shapira, 1997; Slovic, 2000). Following this logic, decision makers in charge of compliance with a rule will avoid rule-violating solutions to organizational strain or slack resources to the extent that they perceive consequences of violating the rule to be negative. Under these new boundary conditions, this underlying proposition on risk works the same in SOIPSVM as in SORVM. Following the logic of SORVM, we propose:

P1: An increase in organizational perceptions of risk associated with violating a rule decreases the likelihood that the organization will violate it.

5.4 Focus of Attention Applied to SOIPVSM

Rather than using focus of attention as a mediating propositional construct as in SORVM, SOIPVISM makes it an overall driving assumption of the model, which we then use to theorize each of the propositions relating contextual conditions and rules characteristics with perceptions of risk. When organizations look for

solutions to performance issues or ways to use slack resources, organizational attention to the issue is limited (March & Simon, 1958), which, in turn, limits the number of decision alternatives (Ocasio, 2002). Although not all alternative solutions will lead to rule violations, studies show that many decision alternatives do lead to violations (Alexander & Cohen, 1996; Harris & Bromiley, 2007). SOIPSVM seeks to explain the factors that affect the likelihood that decision alternatives will result in rule violations.

Moreover, because organizational attention is limited, organizations will focus their attention mainly on rules affecting critical resources or the interests of powerful organizational coalitions (Lehman & Ramanujam, 2009), which occurs because organizations seeking to relieve performance downfalls focus on solutions that involve regaining and maintaining critical resources to survive through the downfall (Pfeffer, 1992). Hence, their focus of attention is less likely to be on security and privacy risks when they have such a myopic focus. These assumptions are consistent with SORVM's focus of attention concept.

5.5 The Role of Economic and Non-economic Strain

SORVM posits that economic strain influences risk perceptions and the likelihood that an organization will violate a rule. SORVM suggests that, when performance falls below the aspiration level, organizations become more risk tolerant and are more likely to violate a rule while searching for a solution to organizational strain resulting from low performance (Lehman & Ramanujam, 2009). However, extremely poor performance, such as when an organization is nearing the point at which it cannot survive, leads to rigidity and risk aversion (Hu et al., 2011b). Similarly, when performance is extremely high, the resulting slack resources decrease the perception of risk associated with searching for new operating methods (Singh, 1986). For example, high-performing or burgeoning organizations, such as Walmart and Groupon, have committed SOX violations due to risky organizational decisions (Rogers, 2012). Thus, we expect both organizations under strain and those with slack resources to engage in risky behavior, which may include rule violations, as they search for solutions to strain or ways to use slack resources.

An organization's performance in relation to other organizations in a particular industry offers a common operationalization of economic strain. An organization's performance relative to a competitor's performance can affect organizational behavior (Harris & Bromiley, 2007; Lant, 1992). Performance is relative to the industry, and one can define or measure it in multiple ways. Financial organizations, for example, are more likely to commit financial fraud insofar as they are low performers in comparison to their competitors. Harris and Bromiley (2007) found that firms that misrepresented their financial statements were more likely to be low performers in comparison to average performers. This finding suggests that low performers might be more likely to violate rules such as those prescribed by SOX. In search of ways to expend slack resources, high-performing organizations may also engage in risky behavior (Singh, 1986).

In addition to economic strain (i.e., organizational performance), SOIPSVM considers non-economic forms of strain. Strain theory suggests that individuals and groups unable to attain their desired goals, whether economic or non-economic, through legitimate means will be more likely to adopt deviant means to do so (Merton, 1938). Examples of non-economic strain include failing to achieve desired status or respect, perceived injustice, the inability to exercise core values, the loss of positive stimuli, and the introduction of negative stimuli (Agnew, 1999, 2001). Non-economic strain creates feelings of deprivation, which prompts individuals and groups to seek solutions to the strain. When legitimate solutions are not available, non-economic strain results in non-compliant behavior (Agnew, 1999).

In relation to privacy and security rules, non-economic strain may result from a conflict between a rule and core organizational values. When rules conflict with core organizational values, the strain may lead organizations to violate the rules in an effort to maintain their core values. Present-day organizations face multiple and competing pressures; consequently, they often select which pressures to succumb to (Kostova et al., 2009). Thus, organizations may choose to violate rules rather than their core values. HIPAA rules provide a clear example of how non-economic strain influences risk perceptions and rule-violating behavior. Some doctors and nurses perceive that HIPAA rules negatively influence the quality and efficiency of patient care (Rivard et al., 2011). Patient care is a core value of the work doctors and nurses perform. The lack of congruence between HIPAA rules and the values of doctors and nurses may lead some medical professionals to violate HIPAA rules even if perceptions of risk are high (Lo et al., 2005). Summarizing this section, we propose:

P2a: Economic strain moderates the relationship between an organization's risk perceptions and its intention to violate an externally governed privacy or security rule.

P2b: Non-economic strain moderates the relationship between an organization's risk perceptions and its intention to violate an externally governed privacy or security rule.

5.6 Contextual Conditions Applied to SOIPVSM

Again, the two major elements of contextual considerations in SORVM are structural secrecy and coupling between violations and outcomes. SOIPVSM embraces violation coupling and explains how it relates to compliance with privacy and security rules. However, SOIPSVM extends SORVM by broadening the scope of structural influences. That is, SOIPSVM proposes that structural secrecy is just one component of organizational communication structures. By broadening the theoretical lens to communication structures, SOIPSVM offers a more holistic and powerful explanation of structural influences on risk perceptions.

5.6.1 Structural Secrecy Applied to SOIPSVM: Organizational Communication Structures

The flow of communication and the organizational structures that facilitate or impede communication flows in organizations influence organizational risk perceptions (Lehman & Ramanujam, 2009; Luhmann, 2005). SORVM suggests that secrecy in organizational communication caused by formal communication structures influences risk perceptions. Formal communication structures are bureaucratic structures, such as hierarchy, centralization, formalization, and specialization, that influence how communication flows through an organization (Miller & Droge, 1986; Van de Ven, 1976). Although secrecy is one aspect of communication structures that influences risk perceptions, other important aspects exist. To broaden the scope of SORVM and offer a more holistic view of the influence of communication structures on risk perceptions, SOIPSVM explains more broadly how communication structures influence risk perceptions. Additionally, SOIPSVM draws attention to the importance of informal communication structures, which receive little attention in SORVM. Informal communication structures are communicative relationships that develop laterally rather than vertically (Ghoshal et al., 1994; Tsai, 2002). We now discuss how communication structures influence organizational risk perceptions.

First, as SORVM posits, secrecy in communication structures decreases risk perceptions. High structural secrecy occurs when the roles and responsibilities for monitoring and complying with a rule are concentrated into one subunit (Kim, Hoskisson, & Wan, 2004). This concentration of rule-related power results from the division of labor, hierarchical structure, or job specialization, all of which isolate the knowledge of rule-related tasks (Vaughan, 1996). Secrecy masks organizational decisions and behavior, which makes non-compliance less detectable while maintaining a façade of compliance (Lehman & Ramanujam, 2009).

Second, communication flows influence the creation of organizational norms (Fiol & Lyles, 1985). Organizational norms can favor compliance or non-compliance with rules (Akers, 2009). Formal and informal organizational structures, such as security training and social support that favors secure behavior, can promote positive security norms and behavior in organizations (D'Arcy et al., 2009; Johnston & Warkentin, 2010). Similarly, adopting common organizational structures can lead to normative tendencies in an entire industry (Kondra & Hinings, 1998). When decision makers deviate from organizational or industry norms, they may experience social pressure and other negative consequences (DiMaggio & Powell, 1983; Kondra & Hinings, 1998). Ultimately, decision makers' anticipating negative outcomes increases risk perceptions (Lehman & Ramanujam, 2009).

Third, organizational communication influences risk perceptions by acting as a surrogate for actual experience (Luhmann, 2005). Direct positive and negative experiences with a rule violation influence risk perceptions (Lehman & Ramanujam, 2009). In a similar way, positive and negative communication about a particular experience can influence the risk perceptions of those who have never had direct exposure to the experience (Luhmann, 2005). Formal structures, such as the division of labor, segregate subunits in organizations such that that each subunit experiences and interprets organizational events differently. At times, decision makers may be required to consider rule-violating behavior without directly knowing the potential outcomes. In such cases, decision makers are likely to rely on the formally and informally communicated organizational beliefs about the outcomes. In such cases, beliefs that draw attention to negative outcomes will increase risk perceptions.

Finally, we cannot ignore informal communication structures. Similar to formal communication structures, informal communication structures affect the transfer of knowledge and the development of norms within organizations (Tsai, 2002). In fact, informal structures can have more influence on communication and knowledge transfer than formal structures (Ghoshal et al., 1994). Information security research also demonstrates the importance of informal structures. For example, scholars have shown informal social

influence to affect security behavior in organizations (Johnston & Warkentin, 2010). More recently, scholars have shown that indirect communication through subtle interface changes may increase employees' perceived accountability to protect the security of organizational systems (Vance et al., 2013, 2015). Given this background, we propose:

P3a: An increase in formal communication structures that favor rule compliance increases organizational perceptions of risk associated with a rule violation.

P3b: An increase in informal communication structures that favor rule compliance increases organizational perceptions of risk associated with a rule violation.

5.6.2 Violation Coupling Applied to SOIPVSM

Due to the current regulatory environment, privacy and security violations may rarely be tightly coupled to negative outcomes. For example, because it is costly and time-consuming to prosecute credit card fraud successfully, few actual court cases have been pursued (Shaw, 2010). Similarly, the regulatory agencies that govern HIPAA and SOX compliance have rarely levied fines. Consequently, SOIPVSM adds some key extensions to violation coupling to better ground in the security/privacy context.

When violation coupling is loose, the outcomes of a violation are ambiguous and not easily predicted, and the perceptions of risk decrease (Lehman & Ramanujam, 2009). The ambiguity resulting from loose coupling drives organizations to interpret outcomes in ways that favor current organizational processes even if these interpretations are not necessarily correct (Weick, 1995). The ability to interpret outcomes in a favorable manner decreases risk perceptions. Organizations often fulfill this need by looking to past actions and relying on previous alternatives for remedying problems (Feldman & Pentland, 2003; March, 1997). Similarly, to validate prior decisions, organizational members may construe outcomes in a self-justifying manner (March, 1997). If an organization has previously violated a rule, the ambiguity caused by loose coupling makes the risk of violating the rule again less discernible (Lehman & Ramanujam, 2009).

Loose coupling may be particularly prevalent in our security/privacy context. To illustrate, we use HIPAA against the backdrop of the industry itself. First, the healthcare industry is complex and highly fragmented (Bentley, Effros, Palar, & Keeler, 2008). Some observers consider it the most complex industry in the world because of its massive size; mix of government (e.g., national, state, regional, local), private for-profit, and private not-for-profit elements; and extreme stakeholder pressures from doctors' organizations, patients, lawyers, regulators, pharmaceutical companies, medical manufacturers, and patients. This complexity and fragmentation makes it difficult for organizational decision makers to relate organizational violations with their associated outcomes correctly because it is difficult to understand the maze of regulations and who may be harmed if the regulations are not followed (Field, 2008). HIPAA is just one of hundreds of regulations that the U.S. medical industry has to worry about, which undermines coupling. In fact, medical regulations are so complex that medical stakeholders often must report to competing, and often conflicting, authorities for guidance (Field, 2008). Second, HIPAA regulations allow organizations to outsource their data storage and other HIPAA-regulated tasks (HHS, 2003). Outsourcing may create loose coupling because violations committed by the outsourcer may not be recognized by the medical organization and organizational memory may not be shared between the outsourcer and the medical organization. Third, the Department of Health and Human Services (HHS) does not monitor HIPAA compliance but asks that victims report abuse (NARA, 2011). If a delay occurs between a HIPAA privacy violation and the time at which a patient reports the abuse or HHS commences an investigation or if the patient never reports the abuse, loose coupling is possible because temporal delays between a violation and its associated outcome may increase loose coupling (Lehman & Ramanujam, 2009). The same may be true for PCI DSS. Because many organizations are left to audit their own compliance (Morse & Raval, 2008), cardholder complaints may be the only indication of non-compliance. Therefore, existing privacy and security compliance systems may have little influence over organizational decision processes due to loose coupling. To address these possibilities in our context, SOIPVSM extends the underlying violation-coupling proposition from SORVM as follows:

P4a: Privacy and security violations loosely coupled to outcomes decrease organizational perceptions of risk despite prior outcomes associated with the rule violation.

P4b: Privacy and security violations tightly coupled to positive outcomes decrease organizational perceptions of risk associated with the rule violation.

P4c: Privacy and security violations tightly coupled to negative outcomes increase organizational perceptions of risk associated with the rule violation.

5.7 Rule Characteristics Applied to SOIPVSM

Again, the three major elements of rule characteristics in SORVM are enforceability, procedural emphasis, and rule connectedness. SOIPVSM improves on this foundation by first conceptualizing enforceability in terms of the deterrence theory concepts of certainty, severity, and celerity of sanctions. SOIPVSM also extends SORVM by examining goal clarity instead of procedural emphasis. Goal clarity offers a broader and richer theoretical lens for understanding how the emphasis of rules influences organizational behavior.

5.7.1 Enforceability Applied to SOIPVSM: Certainty, Severity, and Celerity of Sanctions

To contextualize enforceability, SOIPSVM leverages deterrence theory. SOIPSVM contextualizes enforceability in terms of the certainty, severity, and celerity of the sanctions that an external regulatory body enforces on an organization for its violating an organizational privacy or security rule. Thus, the greater the extent to which an external regulatory body enforces rules with certainty, severity, and celerity, the higher the risk perceptions associated with organizational rule violations. Deterrence theory originates from criminology research, but IS security research has applied it to studies of information security policy compliance (e.g., D'Arcy et al., 2009; Hu et al., 2011a; Siponen & Vance, 2010; Straub, 1990). Deterrence theory posits that the perceptions of sanctions designed to punish violators deter individuals from deviant behavior. Research has examined multiple characteristics of the sanctions used to induce deterrence, which includes their severity, certainty, and celerity. The severity of sanctions refers to “the perceived degree of punishment for [an] intended act” (Hu et al., 2011a, p. 57). The certainty of sanctions refers to “the perceived probability of being punished for [an] intended act” (Hu et al., 2011a, p. 57). The celerity of sanctions refers to “the perceived swiftness of being punished for [an] intended act” (Hu et al., 2011a, p. 57).

Although researchers commonly apply general deterrence theory at the individual level, we argue that general deterrence theory constructs are ideal for SOIPSVM because they conceptualize organizational violations as resulting from the decisions of a few powerful individuals. In cases of high secrecy, decisions to violate rules, although coerced by a leadership collective, may even belong to a single person. Additionally, the assumptions and driving forces underlying perceptions of enforcement are identical in terms of general deterrence and SORVM’s concept of enforceability. Both theories suggest that individuals and small groups react to external pressures in a fearful and compliant way as representatives of the overall organization. Enforceability, as defined previously, is concerned with whether behavior is monitored (i.e., how certain detection and sanction will be) and how damaging the effects will be (i.e., how severe the sanction will be). Hence, deterrence aptly fits our context.

Enforceability is high when regulatory agencies are able to monitor an organization’s actions frequently, which is most likely when the regulatory agency and organization are highly interdependent (Edelman, 1992). Scholars have shown monitoring increases to increase perceptions of sanctions’ certainty and severity of sanctions (D'Arcy et al., 2009). When the likelihood of monitoring is high, enforceability increases the perceived risk of violating a rule by increasing the chances of detection and reducing organizations’ control over the negative consequences of a rule violation (Lehman & Ramanujam, 2009). In contrast, when the likelihood of monitoring decreases, perceptions of risk decrease because organizations are better able to plausibly deny accusations (Gioia, 1992) and can increase control by creating symbolic compliance (Edelman, 1992) but not meaningful compliance.

Presently, the HIPAA and PCI DSS regulating bodies do not directly monitor organizational compliance but instead rely on victims to report violations (NARA, 2011). Any delay in patients’ or consumers’ reporting could decrease the perceptions of celerity. In HIPAA’s case, many reported abuses are resolved even before HHS can start an investigation. When victims are left to report abuses, laws are more likely to be abused than when the rules are monitored by third-party agencies (Miller & Sarat, 1981). Historically, few documented cases of regulatory sanctions for HIPAA violations exist (EMS Insider, 2008). However, with changes to HIPAA regarding regulatory powers, sanctions are more common. Penalties for SOX were also lacking historically. Although the regulatory environment is changing, the lack of previous negative outcomes made HIPAA and SOX penalties appear unlikely and uncertain. However, with increases in sanctioning, risk perceptions are likely to increase. Similarly, with the advent of the HITECH Act, stiff penalties are increasingly common, such as the $1 million fine assessed to Massachusetts General Hospital and the $4.3 million fine assessed to Cignet Health of Prince George’s County, Maryland. These organizations are unlikely to repeat their offenses due to an increase in the perceived risk created by the severe fines and settlements.

Another key issue of sanctions applied in an organizational security/privacy context is that the salience of deterrence efforts will likely vary according to the coalitions involved. For example, accountants steeped in SOX knowledge are more likely to feel deterrence effects from SOX regulations than line production managers who may have little to no knowledge of SOX and the deterrence penalties involved. Deterrence effects can be particularly interesting in a medical context. In hospitals, for example, nurses, doctors, and administrators represent three main subcultures, each with partially separate and partially overlapping values (Rivard et al., 2011). Each group has different views about the organization and about HIPAA violations. In general, administrators feel the greatest need to comply with HIPAA rules, whereas doctors and nurses may see HIPAA rules as hindrances to their daily work given that "it has generated a dizzying set of health-care administrative activities and a new work for legal consultants" (Feld, 2005, p. 1440). HIPAA has overburdened doctors, especially those in private practice, with paperwork and bureaucracy and, consequently, has caused doctors to be less willing to enroll their patients in research protocols that may improve practice and save their patients' lives (Rash, 2008). Another unintended side effect of HIPAA that has negatively affected practice is that it has negatively influenced information sharing that is crucial to improving practice (Davenport, 2013). Not surprisingly, administrators feel a greater self-efficacy to comply than do medical staff (Johnston & Warkentin, 2008). Nurse and doctor subcultures may be more susceptible to privacy/security violations because HIPAA rules and deterrence mechanisms are less salient to their day-to-day jobs than administrators are. To summarize this section, we propose:

P5a: An increase in the certainty of sanctions by an external regulatory body for an organizational privacy or security rule violation increases an organization's perceptions of risk associated with the rule violation.

P5b: An increase in the severity of sanctions by an external regulatory body for an organizational privacy or security rule violation increases an organization's perceptions of risk associated with the rule violation.

P5c: An increase in the celerity of sanctions by an external rule body for an organizational privacy or security rule violation increases an organization's perceptions of risk associated with the rule violation.

5.7.2 Procedural Emphasis Applied to SOIPVSM: Adding Goal Clarity

SORVM posits that rules that focus on procedures rather than desired outcomes will decrease perceptions of risk. This suggestion is based on the premise that procedures allow organizations to signal compliance to governing bodies even when organizational behaviors may be contrary to the rule's intended outcomes (Lehman & Ramanujam, 2009). By framing procedures and outcomes as dichotomous, SORVM assumes that the outcomes of outcome-oriented rules are always clear. However, rule outcomes are not necessarily clear to those expected to follow them (Katz, 2006). For this reason, SOIPSVM re-conceptualizes procedural emphasis as (the lack of) goal clarity. Building on the definition that Tziner, Kopelman, and Livneh (1993) make, we conceptualize goal clarity as the extent to which a rule designates objectives that minimize the potential for alternative interpretation and provides information about how to achieve the objectives.

By examining goal clarity, SOIPSVM does not assume that rules' objectives are equally clear. Goal clarity also broadens SORVM's scope by opening the possibility for other influencing factors besides procedural emphasis. SORVM posits that excessive procedures can obscure the desired outcomes of a rule and leave room for interpreting the rule in different ways (Lehman & Ramanujam, 2009). However, other factors may also influence the clarity of a rule's objectives. For example, using jargon in writing a rule or failing to employ a shared vocabulary can create confusion about rule outcomes. Frequently changing procedures and objectives may also create confusion. By examining goal clarity, SOIPSVM extends the theoretical bounds and explanatory power of the procedural emphasis concept. When a rule's goal clarity is high, the rule clearly defines its expected outcomes. When a rule clearly defines outcomes, ambiguity will be low, which makes plausible deniability less likely and increases perceived risk. Currently, many of HIPAA's rules are flexible and allow for interpretation in that they call for "reasonable" actions (HHS, 2008). Similarly, interpretations of HIPAA rules are continually evolving (Wipke-Tevis & Pickett, 2008). The lack of clarity allows for discretion in decision making efforts, which diminishes the potential influence of external pressures on an organization. PCI DSS also allows organizations to interpret many of its rules openly by allowing them to develop their own policies and procedures for compliance (Owen & Dixon, 2007). As such, organizations commonly misunderstand PCI DSS's purpose (Rees, 2010).

However, PCI DSS contains some rules that are high in goal clarity and others that are low. For example, PCI DSS rules about maintaining firewalls and encrypting transmissions are prescriptive and highly procedural (Morse & Raval, 2008) and, therefore, low in goal clarity (Lehman & Ramanujam, 2009). Although these rules offer information for implementation, they do not offer clear security-related goals. That is, they do not help to explain the rule's expected outcomes.

Other PCI DSS rules are more outcome oriented, such as those related to developing and maintaining secure systems (Morse & Raval, 2008). However, organizations commonly misunderstand these rules (Rees, 2010) possibly because many organizations view PCI DSS compliance as a one-time action or as requiring action only when they are audited. Maintaining secure IS requires continuous monitoring, particularly during system upgrades and maintenance (Kidd, 2008). To summarize this section, we propose:

P6: An increase in the goal clarity of an organizational privacy or security rule increases an organization's perceptions of risk associated with violating the rule.

5.7.3 Rule Connectedness Applied to SOIPVSM

Finally, we assume that rule connectedness works the same in a security/privacy context as it does in a more general organizational context as with SORVM. Thus, SOIPVSM replicates the SORVM proposition that rule connectedness increases risk perceptions.

Many information security and privacy rules, such as those prescribed by HIPAA, have a high rule connectedness, which means that they connect to a large and increasing number of rules. For example, the ubiquity of healthcare IT (HIT) in the healthcare industry prompted legislators to enhance the HIPAA protections by developing the HITECH Act. Legislators created the act to encourage the meaningful use and adoption of HIT (HHS, 2011). The introduction of the HITECH Act may reduce organizations' intentions to violate HIPAA rules because HITECH rules are closely connected with existing HIPAA rules. Following the logic of SORVM, we propose:

P7: An increase in connectedness of organizational privacy or security rules increases an organization's perceptions of risk associated with violating a rule.

6 Discussion

Given the problems that many organizations face about complying with IT privacy and security rules, we propose SOIPSVM, a model developed to explain such organization-level rule violations. In particular, we use HIPAA, PCI DSS, and SOX as examples of externally governed IT privacy and security rules. The model should explain organizational compliance with similar privacy and security rules, such as the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, the Data Privacy Directive (DPD) in Europe, and the Data Protection Act of 1998 in the UK.

6.1 Application of SOIPSVM to the TJX Companies Security-Violation Case

To demonstrate SOIPSVM's potential applicability to organizational security and privacy research, we now apply the entire SOIPSVM model in the broader context of the well-known TJX Companies security-violation case, which the media has extensively reported (Cereola & Cereola, 2011; Chickowski, 2008; Xu, Grant, Nguyen, & Dai, 2008). Xu et al. (2008, p. 575) aptly summarize this case as follows:

> *TJX Companies Inc. is a leading off-price apparel and home fashions retailer with headquarters situated in the United States. In late 2006, the company discovered it was victim to a massive security breach, which compromised millions of customer records. Despite the internal exchanges within the IT department concerning the upgrade of their wireless security standard protocol, the company opted for cost savings rather than increased spending. As the company financials took a hit, the company was faced with pending lawsuits from credit card companies and affected customers; government scrutiny of IT security standards; loss of consumer confidence; among other concerns. Though it has not yet concluded the extent of the financial impact of this incident, analysts estimate the full cost of the breach might amount up to one billion dollars.*

Importantly, this case is considered one of the most catastrophic instances of financial losses suffered by a firm because of intentional violations of security and privacy standards. Specifically, though many reports have considered the TJX case as an example of security breaches by external hackers, we offer a unique perspective by focusing on the organization's rule violations and their antecedents (without which the

security breach could not have happened). SOIPSVM clearly explains these intentional violations. Given this background, we first verify that the TJX case meets SOIPSVM's core assumptions as Table 3 lists. We then assess the degree to which the case facts support or undermine SOIPSVM's core propositions.

6.1.1 TJX and SOIPSVM's Assumptions

We first consider whether the organizational behaviors that led to the TJX security breach constitute external rules that are low in ambiguity and that members of the organization should have known. TJX was using the wired equivalent privacy (WEP) security protocol for wireless transmissions, which had serious security issues known to TJX's IT department and upper management. Its using the WEP protocol was contrary to standards required by PCI DSS. All major card issuers and banks at the time were expected to adopt PCI DSS. Penalties of non-compliance with PCI DSS included fines or the loss of the ability to process credit cards. Nonetheless, TJX intentionally violated PCI DSS to "buy time" to identify a less expensive implementation approach (Xu et al., 2008).

Although the PCI policies were in place, TJX initially failed nine of the 12 requirements that were set; though, without any major penalties, Visa allowed TJX to resume normal operations on the condition that they would improve its security (Chickowski, 2008). At this same time, Chief Information Officer Paul Butka knew that sales had picked up throughout the company and focused on a conservative approach to its internal security investments (p. 580).

Given the clear requirements of PCI DSS and TJX management's decision to ignore security simply to save money, we conclude that TJX knowingly committed a violation of a well-known credit card security standard.

Next, we consider SOIPSVM's organizational assumptions. The first key organizational assumption is that groups with access to critical resources predominantly determine organizational actions. Top management (including the CIO) at TJX had the resources (i.e., money and support) needed to achieve full PCI DSS compliance by upgrading wireless security protocols, but they chose to withhold it to save money. The savings were potentially substantial, and management was clearly making a calculated cost–benefit decision that involved a miscalculation of risk. Implementing PCI DSS compliance requires an average time commitment of three to five years, and the process is highly complex, costly, and time-consuming (Everett, 2009; Rees, 2010).

The second key organizational assumption concerns vulnerable organizations subject to violations due to organizational strain. Strain is readily apparent in the TJX case because it made decision not to better protect its customers in the context of general financial strain.

Finally, TJX's rule violations conform to SOIPSVM's rule-violation assumptions. The violations were not due to the sabotage or misconduct of one individual; they were a broad-based management decision made with the knowledge of potential risks but without an appreciation of their magnitude. Consequently, the rule violations occurred as the result of satisficing solutions arising from limits to organizational attention that presented themselves during the search for solutions to performance issues. That is, the company was under pressure to improve performance, and it saw improving customer security as a cost with no potential upstream revenue; thus, TJX sacrificed security to improve the bottom line.

6.1.2 TJX and SOIPSVM's Mediating Variables

Again, the company's decision not to better protect its customers was a financial decision made in the context of general financial strain. In fact, we discovered that, two months prior to the emails mentioned in Xu et al. (2008), TJX issued a press release that indicated the company was under financial strain. In this document, Bernard (Ben) Cammarata, Chairman, Acting President, and Chief Executive Officer of TJX Companies, stated:

> *September sales trends were softer than we had expected. We attribute this largely to what we believe was consumer malaise in the aftermath of the hurricanes, as well as the negative impact of unseasonably warm weather in the Northeast, Midwest and Canada on the demand for fall fashions.*
>
> *On a broader level, having recently taken on the role of Acting CEO, I intend to lead our great and fundamentally strong company to the success I know we can achieve. To this end, I have set profitable top-line growth as our highest priority* (Lang, 2005).

These quotes show that TJX had not reached projected sales (i.e., aspiration level) and decided to make "profitable top-line growth" its highest priority. Notably, an "acting" CEO who was under personal strain to clean up TJX and turn it around made these statements. In fact, as part of the press conference, TJX announced it was exiting its failing e-commerce business due to strategic blunders and failure to understand the business in general. These facts provide further evidence that the company's decision to violate PCI DSS was financially motivated and related to aspiration levels. Importantly, when performance is at or above the aspiration level, organizations tend to be less risk seeking and are less likely to look for new methods to increase performance (Levinthal & March, 1993).

In summary, TJX was an organization under strain in a highly competitive industry in which it was not a top performer and, thus, fell short of its aspiration level. Worse, most of its competition beat TJX to the rush to e-commerce; TJX adopted e-commerce so slowly that it completely failed and decided to exit this business. Accordingly, the TJX case provides support for P2, which proposes an increased moderation effect between risk and the likelihood of violation, which can eventually lead to actual violation.

6.1.3 TJX and SOIPSVM's Contextual Conditions Propositions

Members of upper management knew they were violating PCI DSS by employing the WEP security protocol. Moreover, after it became widely known that upper management decided to save money rather than protect customers' security, senior IT staffer Lou Julian emailed the CIO and other executives with the following prescient warning, which did not change management's decision (Chickowski, 2008).

> *Saving money and being PCI compliant is important to us, but equally important is protecting ourselves against intruders. Even though we have some breathing room with PCI, we are still vulnerable with WEP as our security key. It must be a risk we are willing to take for the sake of saving money and hoping we do not get compromised* (p. 29).

Another senior IT staffer sent the following email, which also did not result in a change (Chickowski, 2008):

> *The absence of rotating keys in WEP means that we truly are not in compliance with the requirements of PCI. This becomes an issue if this fact becomes known and potentially exacerbates any findings should a breach be revealed* (p. 29).

The privacy commissioner of Canada, one of the investigators of the case, also concluded that TJX knowingly committed a violation. The commissioner concluded:

> *TJX relied on a weak encryption protocol and failed to convert to a stronger encryption standard within a reasonable period of time…. While TJX took the steps to implement a higher level of encryption, there is no indication that it segregated its data so that cardholder data could be held on a secure server while it undertook its conversion to WPA…. If adequate monitoring of security threats was in place, then TJX should have been aware of an intrusion prior to December 2006* (Xu et al., 2008, p. 584).

Given this background, we assert that TJX suffered from weak communication structures that failed to support compliant behavior. The lack of communication in favor of compliance decreased management's perceptions of risk as SOIPSVM proposes. Communication structures that do not support compliance occur when the roles and responsibilities for monitoring and complying with a rule are concentrated into a single subunit (Kim et al., 2004), knowledge of the rules is isolated, (Vaughan, 1996), and the activities of a subunit are dissociated from those of other subunits (March & Simon, 1958). TJX had a double problem in that IT was centralized and left solely in charge of PCI DSS compliance. The lack of communication structures to support compliance communication across organizational subunits decreased risk perceptions. Coupled with this, IT had no real power, budget, or authority to gain the resources necessary to comply with PCI DSS. Such decision making power was relegated to centralized management outside of IT. Notably, the CIO continually sided with management regarding IT concerns and abandoned what should have been a more open role of championing both sides. One example is the satisficing demonstrated in an email the CIO sent to his staff on November 23, 2005, in which he encouraged them to downplay the risk of their situation even though it should have been clear to him that they were not PCI DSS compliant and were at great risk (Chickowski, 2008).

> *We can be PCI compliant without the planned FY '07 upgrade to WPA technology for encryption because most of our stores do not have WPA capability without some changes…. WPA is clearly best practice and may ultimately become a requirement for PCI compliance sometime in the future. I think we have an opportunity to defer some spending from FY '07's budget by removing*

> *the money from the WPA upgrade,* but I would want us all to agree that the risks are small or negligible (p. 29, emphasis added).

When his staff clearly, formally communicated through email warnings that the risks were not small or negligible, he ignored the warnings and pressed forward in support of management's desire to defer IT spending for compliance. He was the one senior member of management who knew better, yet he caved to management pressure. An additional source of structural secrecy with respect to IT was the lack of an IT committee on TJX's board of directors, another aspect of its failure to comply with IT controls standards (Cereola & Cereola, 2011). Hence, one person was able to downplay and obfuscate risk because no one in senior management or on the board of directors had the knowledge to vet his claims. The lack of support in formal communication structures to support PCI DSS compliance (namely, through TJX hierarchy) created low risk perceptions, which supports P3a. The low risk perceptions and rule violation in the TJX case supports P1.

Likewise, because the CIO was the only person with an IT background invited to the frequent discussions of IT budgets, TJX lacked the informal communication (e.g., the open-door ability for an IT staff member to explain the issues in person to senior management) that can decrease structural secrecy. Only the CIO discussed the issues with the IT department. When senior IT staff formally warned upper management of the risks, management deferred to the CIO rather than further communicating with these staff members (P3b supported).

Considering that the members of TJX's top management were not IT or security experts and no major security breaches had occurred up to this point in corporate history, top management easily downplayed the risks involved in its satisficing decision even though staff had warned management of the risks several times. That is, there was no organizational memory of past violations because top management was using inferior security protocols and choosing to roll out improvements slowly in direct violation of PCI DSS. This situation specifically created the unfortunate scenario of prior positive outcomes (no security breaches) with tight coupling, which supports P4 (specifically, 4b). This greatly exaggerated lack of perceived risk led to security violations. Top management believed the oft-repeated mantra that "IT doesn't matter" and that they should minimize IT investment. The fact that the company had strategically failed in its e-commerce business and was in the process of exiting it may have reinforced the attitude that IT is a non-strategic cost center.

6.1.4 TJX and SOIPSVM's Rule Characteristics Propositions

Visa chose not to penalize TJX and allowed the company to continue to violate PCI DSS with TJX's partial implementation of the PCI DSS rules. Moreover, PCI DSS does not involve a governing body that directly monitors organizational compliance but instead relies on victims to report violations (NARA, 2011). Accordingly, the discovery of TJX's violations by credit card companies was uncertain; punishments were highly unlikely, and they lacked severity and swiftness. Hence, the TJX case also supports P5: the lack of sanctions served to diminish perceived risk.

In terms of goal clarity, it would appear that the way to achieve PCI DSS compliance is clear because the rule specifically outlines 12 requirements. However, PCI DSS is complex, and it allows organizations to interpret many of its rules openly by freeing organizations to develop their own policies and procedures for compliance (Owen & Dixon, 2007). Therefore, organizations commonly misunderstand PCI DSS's purpose (Rees, 2010). Consequently, the case supports P6.

Finally, we consider the degree to which PCI DSS exhibits rule connectedness. We believe that the rule connectedness of PCI DSS is moderately low. On one hand, it does have a moderate relationship with SOX in that SOX requires constant monitoring and concerted efforts to design systems compliant with its rules (Mishra & Weistroffer, 2007). Unfortunately, the courts' interpretations of SOX have become increasingly divergent (Lechner, 2012), further obfuscating any connection between SOX and PCI DSS. Moreover, one can argue for rule connectedness to Federal Trade Commission (FTC) laws by citing the fact that TJX violated the FTC Act by not providing "reasonable" security for personal information. Thus, the key problem we see with PCI DSS connectedness to other laws/regulations is its highly technical and industry-specific nature, which led to TJX's decreased ability to estimate risk accurately. Thus, we conclude that the relationship between rule connectedness and perceived risk, as proposed in SORVM and assumed in SOIPSVM, is not well supported (P7 supported). Table 4 summarizes the propositions supported by the TJX case.

6.2 Contribution of SOIPSVM to Theory and Research

SOIPSVM contributes to theories of organizational deviance in five ways. First, SOIPSVM introduces the concept of selectivity in rule violations to privacy and security research, a research area in need of organization-level theories. This concept can improve privacy and security research by showing that organizational violations of privacy and security rules are dynamic and selective yet influenced by external forces.

Second, SOIPSVM proposes that selective rule violations may extend beyond organizations under strain, such as economic hardship. Slack resources may also lead to risky organizational behavior that could result in rule violations. Thus, SOIPSVM is applicable both to organizations seeking to remedy poor performance and those seeking ways to use slack resources. Further, SOIPSVM more completely explains the way organizational performance influences deviant behavior. Drawing on research on organizational aspiration levels (Hu et al., 2011b), we propose that organizations are likely to disregard external pressures to conform to regulations only when their performance is extremely high or moderately low in comparison to their aspiration levels. SORVM considers the effects of performance only when it is below organizational aspiration levels, which fails to benefit from the nuanced insights of recent research on organizational aspirations. SOIPSVM includes organizational performance relative to an aspiration level as a moderating variable. Notably, aspiration levels were a clear factor in the TJX case.

Table 4. Propositions Supported by the TJX case

Proposition	Supported?	Evidence
P1. Risk perceptions decrease rule violations	Yes	TJX email correspondence shows low risk perceptions among top managers, which resulted in a violation of PCI DSS
P2a. Economic organizational strain moderates an organization's risk perceptions and its intention to violate rules.	Yes	TJX faced financial strain at the time of the violation. TJX stated that improving their financial situation was the highest priority. (There was not enough evidence to support non-economic strain for P2b, although it was likely present).
P3a. Formal communication structures that favor compliance increase risk perceptions.	Yes	Formal hierarchy did not support PCI DSS compliance as a priority. Internal monitoring and compliance decisions were isolated to the IT department. (There was not enough evidence support informal communication structure for P3b).
P4b. Privacy and security violations tightly coupled to positive outcomes will decrease organizational perceptions of risk associated with the rule violation.	Yes	TJX had not experienced prior negative outcomes related to using WEP and received no prior penalties for lack of PCI DSS compliance. There is not enough information to support P4a and P4c.
P5. Certainty (a), severity (b), and celerity (c) of sanctions increase risk perceptions.	Yes	The lack of monitoring and lack of swift, certain, and severe penalties from the payment card industry created low perceptions of risk among TJX management. They were essentially given carte blanche to continue the status quo with no penalty.
P6. Goal clarity of a rule increases risk perceptions.	Yes	In many instances, PCI DSS is open to interpretation.
P7. Rule connectedness increases risk perceptions.	Yes	There are few rules related directly to PCI DSS. In communication between management, no other rules were mentioned.

Third, SOIPSVM includes considerations of non-economic conceptualizations of risk and organizational strain. SORVM considers mainly economic strain and perceptions of economic risk. Drawing from non-economic conceptualizations of perceived risk (Dinev & Hart, 2006), SOIPSVM suggests that risk can be based on threats to values and other important organizational concerns in addition to economic threats. Similarly, strain theory is not limited to economic strain (Merton, 1938). Strain may arise any time an individual or collective cannot achieve a goal or satisfy a value through legitimate means. For example, one can perceive privacy laws in medical settings as a threat to patient care. Where one perceives privacy rules to affect patient wellbeing negatively, organizations may feel strain and choose rule-violating solutions to

remedy the strain. By extending SORVM in this way, SOIPSVM broadens the scope of selective organizational violations to include a wider set of circumstances.

Fourth, SOIPSVM increases the explanatory power of two constructs from SORVM; namely, structural secrecy and procedural emphasis. SOIPSVM introduces formal and informal communication structures instead of structural secrecy and a rule's goal clarity instead of procedural emphasis. The TJX case supports both of these extensions. Formal and informal communication structures that support compliant behavior more richly explain risk perceptions than structural secrecy alone in part because structural secrecy is just one aspect of communication structures. We highlight other important aspects of communication structures that relate to risk perceptions, such as the norm-setting powers of communication structures and the ability of organizational communication to act as a surrogate for actual experience. Goal clarity extends procedural emphasis by highlighting the false assumption that outcome-oriented rules are always clear. Goal clarity broadens the theoretical lens of procedural emphasis by drawing attention to other aspects of rules beyond an emphasis on procedures that influence risk perceptions.

Fifth, we identify how one can extend general deterrence constructs to organization-level research. SOIPSVM posits that organizational behavior results from a few powerful decision makers acting in their legitimate organizational appointments and working to achieve organizational goals. Because SOIPSVM deals with the perceptions of a few powerful individuals, one can adapt individual-level constructs such as perceived certainty, severity, and celerity of sanctions to account for organizational behavior, which is particularly illuminating for the TJX case because the company knowingly violated PCI DSS but was lightly reprimanded by Visa even though it could have been fined and subjected to further sanctions. We argue that such weak sanctions essentially rewarded TJX for its neglect and, thus, undermined the sanctioning authority of PCI DSS. Had Visa severely fined and punished TJX, the company's calculations of sanctions and risk may have changed, which may have prevented the security breach.

We believe SOIPSVM can ultimately help to inform both the creation and reform of privacy and security rules and the structuring of the regulatory environments that govern these rules. Moreover, SOIPSVM offers insight into ways organizations can structure themselves to reduce violations and increase corporate social responsibility.

6.3 Implications for Practice

In view of each of our model's propositions, we offer several suggestions for structuring organizations and regulatory environments. In essence, managers, stakeholders, and investors can use SOIPVISM as a warning guide in assessing a company's potential for highly damaging rule violations. SOIPVISM not only is a novel assessment guide but also points to structural reforms that organizations can implement to increase risk perceptions and decrease violations. It can also serve as a guide for regulating authorities in their search for ways to increase participation in and compliance with their regulations.

For example, organizations and regulatory bodies should be concerned with inducing and increasing organizations' perceptions of risk related to privacy and security rule violations. Organizational communication structures can strongly influence risk perceptions. Regulators might develop policies to mandate multiunit teams in organizations, which would include organizational members from different organizational functions, to govern decisions about privacy and security rules. Multi-unit compliance teams may increase risk perceptions by decreasing structural secrecy and allowing compliance norms to spread throughout the organization. Regulators should also focus more on the core values of organizations that will be subject to privacy and security laws. Organizations with values that conflict with certain rules may be unwilling to follow them (Lo et al., 2005). Therefore, to develop successful regulations, regulators should incorporate core organizational values into their rules. Some privacy and security rules, such as those prescribed by HIPAA, do not adequately consider core values of key organizational coalitions (Rivard et al., 2011).

Managers should also be proactive about developing structures to decrease the likelihood that their organization will violate rules. Managers can institute multiunit compliance teams by assigning members from different organizational units to monitor rule compliance and make decisions regarding issues that pertain to privacy and security rules. Multi-unit teams may ensure compliance with privacy and security standards when under conditions of strain or excess. Managers can also embed in IS the values that align with the external rules governing the organization. Managers should also be cognizant of rule-breaking routines. Past rule-breaking behaviors may continue if organizations do not adjust the rule-breaking status quo. Managers should conduct internal and external audits of their organizations to ensure compliance with privacy and security rules. Audits are likely to decrease structural secrecy and increase risk perceptions.

Through consistent sanctions, regulatory agencies can create the perception that penalties for rule violations are severe, certain, and swift. In terms of regulating bodies, we saw that Visa did not punish TJX for lack of compliance with PCI DSS even though it could have fined TJX for non-compliance. Instead, Visa coddled TJX and allowed it to continue with inadequate security measures, which served to undermine the effect of any potential sanctions, decrease risk, and reward TJX for non-compliant behavior. This case serves as a warning to regulatory agencies that rules prohibiting violations lose their deterrent effect when agencies fail to impose sanctions.

Regulating bodies may need to be more diligent in enforcing the privacy and security rules they govern. Many of the rules we examine in this paper, such as those prescribed by HIPAA and PCI DSS, have not been heavily monitored, and few penalties and fines have been imposed. For example, another flaw of PCI DSS uncovered in the TJX case is that the regulatory agency relied on consumers, who occupy a position of low power and low information, to report violations. Where privacy and security rules are associated with few and inconsistent penalties, organizations are not likely to perceive risk in violating the rules.

Moreover, for some privacy and security laws, fines and penalties have not been assessed because of the laws' complexity and wording. For example, the courts' interpretations of SOX have become increasingly divergent (Lechner, 2012), which undermines perceptions of sanctions and risks for SOX non-compliance. Worse, it makes SOX compliance a guessing game. Similarly, organizations may be subject to penalties under PCI DSS even when they are highly compliant with the primary recommendations in PCI DSS. These inconsistencies in the laws and standards create room for confusion and organizational interpretation. Lawmakers should also consider the reasonableness of the laws for different types of organizations. For example, complying with externally governed rules may be too costly for small organizations and consequently lead to rule violations. Lawmakers do not always consider the economic and non-economic strain exerted by laws. They could adjust such rules based on organizational factors, including size and ability to comply.

Regulatory bodies that govern similar rule domains should band together to leverage their combined power to protect privacy and ensure security. Organizations' perceptions that they could be caught and punished for violating a rule may increase to the extent that multiple related rules govern organizational behavior (Lehman & Ramanujam, 2009). For example, organizations may not violate privacy rules and laws concerning healthcare information if governing bodies besides HIPAA introduced related rules. The American Medical Association, a prominent medical coalition in the US, could adopt privacy standards tied to medical licensure. This redundancy in regulation and the increased penalties for rule violations would likely increase the perceived risk of abusing healthcare information.

6.4 Limitations and Future Research

SOIPSVM's primary limitation is that it no one has yet empirically tested it. To help researchers test SOIPSVM, we briefly discuss ways that they could operationalize and test its constructs. Multiple measures exist for the severity, certainty, and celerity of sanctions; centralization; and informal communication. Other constructs (e.g., structural secrecy and violation coupling) do not have explicit measures in the literature, which makes operationalization more challenging. Thus, using discretion is pivotal in selecting the most appropriate and representative measures to maximize construct validity. Appendix B suggests alternative measures for all constructs in SOIPSVM.

Another limitation of SOIPSVM is its lack of explanatory power with regard to organizations performing at or above their aspiration levels. Again, part of SOIPSVM's foundation is Merton's strain theory (1938), which SOIPSVM leverages to suggest that organizations that cannot achieve socially desirable goals through legitimate means might seek to do so through deviant behavior. Thus, this theoretical foundation limits the explanatory power of our model to apply to those organizations more likely to commit deviant behavior; that is, those that have not attained their aspiration level. SOIPSVM is also restricted to explaining externally formalized rules. SOIPSVM does not account for violations of informal rules, such as social norms and industry best practices related to privacy and security. Information sharing in supply chain relationships offers an interesting area for studying informal rules because formalized rules do not protect many forms of information exchanged in supply chain relationships. SOIPSVM also cannot explain violations of internally developed employee regulations. The nuances in the differences between externally and internally developed rules and regulations would likely pose a problem in testing the selectivity of rule violations at an organizational level (Lehman & Ramanujam, 2009).

SORVM suggests that organizational attention is an important mediating construct in explaining violations, but the evidence for and discussion of the focus of attention concept is scant in Lehman and Ramanujam's (2009) seminal work. For this reason, SOIPSVM does not apply focus of attention as a construct but instead uses the concept as an axiom to describe certain aspects of the model. Future research could revisit and further develop the role of organizational attention in SOIPVSM.

Although we focus on some externally governed rules in the healthcare, consumer, and financial industries in this paper, researchers can likely extend SOIPSVM to other related domains. SOIPSVM's core assumptions are the primary constraints that researchers should consider in developing such an extension. Nonetheless, further theoretical development could neutralize many of the limiting assumptions. For example, researchers could likely apply many of SOIPSVM's concepts to an individual context by substituting individual-level psychological theories for organizational theories.

It would also be useful to study organizations from different cultures and with different HIPAA-like regulations. A study of SOIPSVM focused on a hospital's organizational culture could also be useful because researchers have shown the interplay between doctors, nurses, and administrators to be important in daily hospital life (Rivard et al., 2011).

Finally, it could be beneficial to study SOIPSVM in the context of multiple privacy laws. For example, one could examine HIPAA, PIPEDA, and DPD together to determine whether the rule characteristics or contextual conditions of the laws affect the frequency or severity of violations. Importantly, future studies could also investigate HIPAA violations in relation to mobile technology because many current uses of mobile technology by doctors and nurses represent breaches of HIPAA rules.

7 Conclusion

The explosive growth of HIT in the healthcare industry, credit card transactions in the retail industry, and finance scandals in the financial services industry demonstrates the need for organizations to improve compliance with privacy and security rules. Unless regulatory environments and organizational structures change for the better, rules violations are likely to worsen. SOIPSVM offers a way to explain organizational violations of IT privacy and security rules, such as those prescribed by HIPAA, PCI DSS, and SOX. Our model shows how organization and rule characteristics affect organizations' risk perceptions, which, in turn, result in organizations' deciding to violate rules while under strain. The model and recommendations presented in this paper could help to improve regulatory environments and organizational structures by identifying the deficiencies and vulnerabilities in organizational systems.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). *Is there a cost to privacy breaches? An event study.* Paper presented at the International Conference on Information Systems, Milwaukee, WI.

Agnew, R. (1999). A general strain theory of community differences in crime rates. *Journal of Research in Crime and Deliquency, 36*(2), 123-155.

Agnew, R. (2001). Building on the foundation of general strain theory: Specifying the types of strain most likely to lead to crime and delinquency. *Journal of Research in Crime and Deliquency, 38*(4), 319-361.

Agranoff, M. A. (1991). Controlling the threat to personal privacy. *Information Systems Management, 8*(3), 48-53.

Akers, R. L. (2009). *Social learning and social structure: A general theory of crime and deviance*. New Brunswick, NJ: Transaction Publishers.

Alexander, C. R., & Cohen, M. A. (1996). New evidence on the origins of corporate crime. *Working Papers, U.S. Department of Justice-Antitrust Division, 17*(4), 421-435.

Anton, A. I., He, Q., & Baumer, D. L. (2004). Inside JetBlue's privacy policy violations. *IEEE Security & Privacy, 2*(6), 12-18.

Ariss, S. S. (2002). Computer monitoring: Benefits and pitfalls facing management. *Information & Management, 39*(7), 553-558.

Ashforth, B. E., & Anand, V. (2003). The normalization of corruption in organizations, In B. M. Staw & R. M. Kramer (Eds.), *Research in organizational behavior* (Vol. 25, pp. 1-52). Greenwich, CT: JAI.

Ashforth, B. E., Gioia, D. A., Robinson, S. L., & Treviño, L. K. (2008). Introduction to special topic forum: Re-viewing organizational corruption. *Academy of Management Review, 33*(3), 670-684.

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

Beck, N., & Kieser, A. (2003). The complexity of rule systems, experience, and organizational learning. *Organization Studies, 24*(5), 793-814.

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 36*(4), 1017-1041.

Bennasi, P. (1999). TRUSTe: An online privacy seal program. *Communications of the ACM, 42*(2), 56-59.

Bentley, T. G. K., Effros, R. M., Palar, K., & Keeler, E. B. (2008). Waste in the U.S. healthcare system: A conceptual framework. *Milbank Quarterly, 86*(4), 629-659.

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

Brief, A. P., Buttram, R. T., & Dukerich, J. M. (2000). Collective corruption in the corporate world: Toward a process model. In M. E. Turner (Ed.), *Groups at work: Advances in theory and research* (pp. 471-499). Hillsdale, NJ: Lawrence Erlbaum Associates.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-A527.

Calabresi, M. (2011). Bad deal. *Time.* Retrieved from http://www.time.com/time/magazine/article/0,9171,2101042,00.html

Cereola, S. J., & Cereola, R. J. (2011). Breach of data at TJX: An instructional case used to study COSO and COBIT, with a focus on computer controls, data security, and privacy legislation. *Issues in Accounting Education, 26*(3), 521-545.

Chickowski, E. (2008). Preventing another TJX. *Baseline, 81*, 22-37.

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

Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy, 19*(1), 20-26.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323-343.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *MIS Quarterly, 33*(4), 673-687.

CULS. (2012). 18 USC § 1350—failure of corporate officers to certify financial reports. Retrieved from http://www.law.cornell.edu/uscode/text/18/1350

Cyert, R. M., & March, J. G. (1963). *A behavioral theory of the firm*. Englewood Cliffs, NJ: Prentice Hall.

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

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

Davenport, R. (2013). Report: HIPAA is a hindrance to health care info sharing. *FCW: The Business of Federal Technology*. Retrieved from http://fcw.com/articles/2013/12/03/bpc-hipaa-health-info-sharing.aspx

Desai, M. S., Richards, T. C., & Desai, K. J. (2003). E-commerce policies and customer privacy. *Information Management & Computer Security, 11*(1), 19-27.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

Dhillon, G., & Moores, T. T. (2001). Internet privacy: Interpreting key issues. *Information Resources Management Journal, 14*(4), 33-37.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293-314.

DiMaggio, P., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147-160.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.

Edelman, L. B. (1992). Legal ambiguity and symbolic structures: Organizational mediation of civil rights law. *American Journal of Sociology, 97*(6), 1531-1576.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review, 14*(1), 57-74.

EMS Insider. (2008). Related to: HIPAA privacy rule: 33,000 complaints, no fines. *Optometry, 79*(7), 405-407.

Everett, C. (2009). PCI DSS: Lack of direction or lack of commitment. *Computer Fraud and Security, 2009*(12), 18-20.

Feld, A. D. (2005). The health insurance portability and accountability act (HIPAA): Its broad effect on practice. *American Journal Gastroenterology, 100*(7), 1440-1443.

Feldman, M. S., & Pentland, B. T. (2003). Reconceptualizing organizational routines as a source of flexibility and change. *Administrative Science Quarterly, 48*(1), 94-118.

Feldman, S. S., & Horan, T. A. (2011). The dynamics of information collaboration: A case study of blended IT value propositions for health information exchange in disability determination. *Journal of the Association for Information Systems, 12*(2), 189-207.

Field, R. I. (2008). Why is health care regulation so complex? *Pharmacy and Therapeutics, 33*(10), 607-608.

Fiol, C. M., & Lyles, M. A. (1985). Organizational learning. *Academy of Management Review, 10*(4), 803-813.

Friedman, B. A., & Reed, L. J. (2007). Workplace privacy: Employee relations and legal implications of monitoring employee e-mail use. *Employee Responsibilities and Rights Journal, 19*(2), 75-83.

Fuller, S. R., Edelman, L. B., & Matusik, S. F. (2000). Legal readings: Employee interpretation and mobilization of law. *Academy of Management Review, 25*(1), 200-216.

Ghoshal, S., Korine, H., & Szulanski, G. (1994). Interunit communication in multinational corporations. *Management Science, 40*(1), 96-110.

Gioia, D. A. (1992). Pinto fires and personal ethics: A script analysis of missed opportunities. *Journal of Business Ethics, 11*(5-6), 379-389.

Greco, J. (2001). Privacy: Whose right is it anyhow? *Journal of Business Strategy, 22*(1), 32-35.

Greenaway, K. E., & Chan, Y. E. (2005). Theoretical explanations for firms' information privacy. *Journal of the Association for Information Systems, 6*(6), 171-198.

Harris, J., & Bromiley, P. (2007). Incentives to cheat: The influence of executive compensation and firm performance on financial misrepresentation. *Organizational Science, 18*(3), 350-367.

Henderson, S. C., & Snyder, C. A. (1999). Personal information privacy: Implications for MIS managers. *Information & Management, 36*(4), 213-220.

HHS. (2003). *Summary of the HIPAA privacy rule.* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

HHS. (2008). *Resolution agreement.* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/providenceresolutionagreement.html

HHS. (2011). *HITECH act enforcement interim final rule.* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

Hooper, T., & Vos, M. (2009). Establishing business integrity in an online environment: An examination of New Zealand web site privacy notices. *Online Information Review, 33*(2), 343-361.

Hsu, J., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research, 26*(2), 345-366.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011a). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54-60.

Hu, S., Blettner, D., & Bettis, R. A. (2011b). Adaptive aspirations: Performance consequences of risk preferences at extremes and alternative references groups. *Strategic Management Journal, 32*(13), 1426-1436.

Jafar, M. J., & Abdullat, A. (2009). Exploratory analysis of the readability of information privacy statement of the primary social networks. *Journal of Business, 7*(12), 123-142.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management, 1*(12), 45-71.

Johnson, C., Dowd, T. J., & Ridgeway, C. L. (2006). Legitimacy as a social process. *Annual Review of Sociology, 32*, 53-78.

Johnston, A. C., & Warkentin, M. (2008). Information privacy compliance in the healthcare industry. *Information Management & Computer Security, 16*(1), 5-19.

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

Katz, D. (2006). The motivational basis of organizational behavior. *Behavioral Science, 9*(2), 131-146.

Kidd, R. (2008). Counting the cost of non-compliance with PCI DSS. *Computer Fraud and Security, 2008*(11), 13-14.

Kim, H., Hoskisson, R. E., & Wan, W. P. (2004). Power dependence, diversification strategy, and performance in keiretsu member firms. *Strategic Management Journal, 25*(7), 613-636.

Kondra, A. Z., & Hinings, C. R. (1998). Organizational diversity and change in institutional theory. *Organization Studies, 19*(5), 743-767.

Kostova, T., Roth, K., & Dacin, M. T. (2009). Theorizing on MNCs: A promise for institutional theory. *Academy of Management Review, 34*(1), 171-173.

Kraut, R. E., Fish, R. S., Root, R. W., & Chalfonte, B. L. (2002). Informal communication in organizations: Form, function, and technology, In I. S. Oskamp & S. Spacapan (Eds.), *Human reactions to technology: The claremont symposium on applied social psychology*. Beverly Hills, CA: Sage Publications.

Lang, S. (2005). The TJX Companies, Inc. Reports September 2005 sales; announces exit from e-commerce business; updates earnings outlook for second half of 2005 (press release). *Business Wire*. Retrieved from http://www.businesswire.com/news/home/20051006005419/en/TJX-Companies-Reports-September-2005-Sales-Announces

Lange, D. (2008). A multidimensional conceptualization of organizational corruption control. *Academy of Management Review, 33*(3), 710-729.

Lant, T. K. (1992). Aspiration level adaptation: An empirical exploration. *Management Science, 38*(5), 623-644.

Lechner, J. P. (2012). DOL, courts' interpretations of SOX grow more divergent. *National Law Review*. Retrieved from http://www.natlawreview.com/article/dol-courts-interpretations-sox-grow-more-divergent

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

Leon, L., Abraham, D., & Kalbers, L. (2010). Beyond regulatory compliance for spreadsheet controls: A tutorial to assist practitioners and a call for research. *Communications of the Association for Information Systems, 27*, 541-560.

Levinthal, D. A., & March, J. G. (1993). The myopia of learning. *Strategic Management Journal, 14*(S2), 95-112.

Lewis, B. R., Templeton, G. F., & Byrd, T. A. (2005). A methodology for construct development in MIS research. *European Journal of Information Systems, 14*(4), 388-400.

Lin, H.-F. (2006). Interorganizational and organizational determinants of planning effectiveness for Internet-based interorganizational systems. *Information & Management, 43*(4), 423-433.

Lo, B., Dornbrand, L., & Dubler, N. N. (2005). HIPAA and patient care: The role for professional judgment. *Journal of the American Medical Association, 293*(14), 1766-1771.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal, 25*(5), 433-463.

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal, 25*(3), 193-230.

Lowry, P. B., Posey, C., Roberts, T. L., & Bennett, R. J. (2014). Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. *Journal of Business Ethics, 121*(3), 385-401.

Luhmann, N. (2005). *Risk: A sociological theory* (R. Barrett, Trans.). Chicago: Aldine Transaction.

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

March, J. G. (1997). Understanding how decisions happen in organizations. In Z. Shapira (Ed.), *Organizational decision making* (9-32). New York, NY: Cambridge University Press.

March, J. G., Schulz, M., & Zhou, X. (2000). *The dynamics of rules: Change in written organizational codes*. Palo Alto, CA: Stanford University Press.

March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science, 33(*11), 1404-1418.

March, J. G., & Shapira, Z. (1992). Variable risk preferences and the focus of attention. *Psychological Review, 99*(1), 172-183.

March, J. G., & Simon, H. A. (1958). *Organizations*. Oxford, UK: Wiley.

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review, 3*(5), 672-682.

Miller, D., & Droge, C. (1986). Psychological and traditional detriments of structure. *Administrative Science Quarterly, 31*(4), 539-560.

Miller, R. E., & Sarat, A. (1981). Grievances, claims, and disputes: Assessing the adversary culture. *Law and Society Review, 15*(3-4), 525-566.

Milne, G. R., & Culnan, M. J. (2002). Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 U.S. web surveys. *Information Society, 18*(5), 345-359.

Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy, 25*(2), 238-249.

Mishra, S., & Weistroffer, H. R. (2007). A framework for integrating Sarbanes-Oxley compliance into the systems development process. *Communications of the Association for Information Systems, 20*, 712-727.

Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing, 19*(1), 54-61.

Miyazaki, A. D., & Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. *Journal of Consumer Affairs, 36*(1), 28-49.

Moores, T. T., & Dhillon, G. (2003). Do privacy seals in e-commerce really work? *Communications of the ACM, 46*(12), 265-272.

Morse, E. A., & Raval, V. (2008). PCI DSS: Payment card industry data security standards in context. *Computer Law & Security Report, 24*(6), 540-554.

NARA. (2011). *Electronic code of federal regulations—title 45*. Retrieved from http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=78dff1c5c9198f68cadfc53895bb373d&rgn=div6&view=text&node=45:1.0.1.3.75.4&idno=45

Nord, G. D., & McCubbins, T. F. (2006). Privacy, legislation, and surveillance software. *Communications of the ACM, 49*(8), 73-78.

Ocasio, W. (1997). Towards an attention-based view of the firm. *Strategic Management Journal, 18*, 187-206.

Ocasio, W. (2002). Organizational power and dependence, In J. C. Baum (Ed.), *Companion to organizations* (pp. 263-285). Oxford, UK: Blackwell.

Owen, M., & Dixon, C. (2007). A new baseline for cardholder security. *Network Security, 2007*(6), 8-12.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101-134.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go. *MIS Quarterly, 35*(4), 977-988.

Pavlou, P. A., & Geffen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research, 15*(1), 37-59.

Peslak, A. R. (2005). Internet privacy policies: A review and survey of the Fortune 50. *Information Resources Management Journal, 18*(1), 29-41.

Peslak, A. R. (2006). Internet privacy policies of the largest international companies. *Journal of Electronic Commerce in Organizations, 4*(3), 46-62.

Pfeffer, J. (1992). *Managing with power: Politics and influence in organizations*. Boston, MA: Harvard Business School Press.

Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations*. New York, NY: Harper & Row.

Pinto, J., Leana, C., & Pil, F. (2008). Corrupt organizations or organizations of corrupt individuals? Two types of organization-level corruption. *Academy of Management Review, 33*(3), 685-709.

Pollach, I. (2007). What's wrong with online privacy policies? *Communications of the ACM, 50*(9), 103-108.

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

Rash, M. C. (2008). HIPAA hindrance: Health care privacy act has its fair share of critics and issues. *Triad Business Journal.* Retrieved from http://www.bizjournals.com/triad/stories/2008/07/14/focus1.html ?page=all

Rees, J. (2010). The challenges of PCI DSS compliance. *Computer Fraud & Security, 2010*(12), 14-16.

Rivard, S., Lapointe, L., & Kappos, A. (2011). An organizational culture-based theory of clinical information systems implementation in hospitals. *Journal of the Association for Information Systems, 12*(2), 123-162.

RNCOS. (2011a). *Australian healthcare IT analysis.* Retrieved from http://www.marketresearch.com/RNCOS-v3175/Australian-Healthcare-2683966/

RNCOS. (2011b). *Russia IT industry analysis.* Retrieved from http://www.marketresearch.com/RNCOS-v3175/Russia-6083721/

RNCOS. (2011c). *US healthcare IT market analysis*. Retrieved from http://www.marketresearch. com/RNCOS-v3175/Healthcare-6285506/

Rogers, M. (2012). Sarbanes-Oxley 10 years later: Boards are still the problem. *Forbes*. Retrieved from http://www.forbes.com/sites/frederickallen/2012/07/29/sarbanes-oxley-10-years-later-boards-are-still-the-problem/

Ryker, R., Lafleur, E., McManis, B., & Cox, K. C. (2002). Online privacy policies: An assessment of the Fortune e-50. *Journal of Computer Information Systems, 42*(4), 15-20.

Schein, V. E. (1977). Individual privacy and personnel psychology: The need for a broader perspective. *Journal of Social Issues, 33*(3), 154-168.

Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information & Management, 43*(7), 805-820.

Sewell, G., & Barker, J. R. (2001). Neither good, nor bad, but dangerous: Surveillance as an ethical paradox. *Ethics and Information Technology, 3*(3), 181-194.

Shapira, Z. (1997). *Organizational decision making*. New York, NY: Cambridge University Press.

Shaw, A. (2010). Data breach: From notification to prevention using PCI DSS. *Columbia Journal of Law and Social Problems, 43*(4), 517-562.

Singh, J. (1986). Performance, slack, and risk taking in organizational decision making. *Academy of Management Journal, 29*(3), 562-585.

Sipior, J. C., Ward, B. T., & Rainone, S. M. (1998). Ethical management of employee email privacy. *Information Systems Management, 15*(1), 41-48.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-A412.

Slovic, P. (2000). *The perception of risk*. London, UK: Earthscan.

Smith, J. (1993). Privacy policies and practices: Inside the organizational maze. *Communications of the ACM, 36*(12), 104-104.

Smith, J. (2003). *Sarbanes-Oxley and the need to audit your IT processes*. Retrieved from http://www.cmcrossroads.com/sites/default/files/article/file/2013/XUS4853274file1_0.pdf

Smith, J. H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1015.

Storey, V. C., Kane, G. C., & Schwaig, K. S. (2009). The quality of online privacy policies: A resource-dependency perspective. *Journal of Database Management, 20*(2), 19-37.

Straub, D. W., Jr. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Sullivan, B. N. (2010). Competition and beyond: Problems and attention in the organizational rulemaking process. *Organization Science, 21*(2), 432-450.

Tsai, W. (2002). Social structure of "coopetition" within a multiunit organization: Coordination, competition, and intraorganizational knowledge sharing. *Organization Science, 13*(2), 179-190.

Tziner, A., Kopelman, R. E., & Livneh, N. (1993). Effects of performance appraisal format on perceived goal characteristics, appraisal process satisfaction, and changes in rated job performance: A field experiment. *Journal of Psychology, 127*(3), 281-291.

Van de Ven, A. H. (1976). A framework for organizational assessment. *Academy of Management Review, 1*(1), 64-78.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems, 29*(4), 263-289.

Vance, A., Lowry, P. B., & Eggett, D. (2015). A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *MIS Quarterly, 39*(2), 345-366.

Vaughan, D. (1996). *The challenger launch decision: Risky technology, culture, and deviance at NASA*. Chicago, IL: University of Chicago Press.

Vaughan, D. (1999). The dark side of organizations: Mistake, misconduct, and disaster. *Annual Review of Sociology, 25*, 271-305.

Vaughan, D. (2002). Criminology and the sociology of organizations: Analogy, comparative social organization, and general theory. *Crime, Law & Social Change, 37*(2), 117-136.

Walczuch, R. M., Singh, S. K., & Palmer, T. S. (1995). An analysis of the cultural motivations for transborder data flow legislation. *Information Technology and People, 8*(3), 37-57.

Walczuch, R. M., & Steeghs, L. (2001). Implications of the new EU directive on data protection for multinational corporations. *Information Technology and People, 14*(2), 142-162.

Weick, K. (1995). *Sensemaking in organizations*. Thousand Oaks, CA: Sage Publications.

Whetten, D., Felin, T., & King, B. (2009). The practice of theory borrowing in organizational studies: Current issues and future directions. *Journal of Management, 35*(3), 537-563.

Whetten, D. A. (2009). An examination of the interface between context and theory applied to the study of Chinese organizations. *Management and Organization Review, 5*(1), 29-55.

Wipke-Tevis, D. D., & Pickett, M. A. (2008). Impact of the health insurance portability and accountability act on participant recruitment and retention. *Western Journal of Nursing Research, 30*(1), 39-53.

Xu, W., Grant, G., Nguyen, H., & Dai, X. (2008). Security breach: The case of TJX Companies, Inc. *Communications of the Association for Information Systems, 23*, 575-590.

Zhou, X. (1993). The dynamics of organizational rules. *American Journal of Sociology, 98(*5), 1134-1166.

Appendix A: Supplemental Information on HIPAA, PCI DSS, and SOX

HIPAA

In the United States, HIPAA and the associated Health Information Technology for Economic and Clinical Health (HITECH) Act, governed by the Department of Health and Human Services, have assumed the role of guarding protected health information (PHI). In other parts of the world, single laws protect PHI and other types of private consumer information. For example, Canada's Personal Information Protection and Electronic Documents Act establishes guidelines for protecting the electronic distribution of all types of private data, including PHI. The same is true for the Data Protection Directive in the European Union.

In recent years, healthcare IT (HIT) has become essential in the healthcare industry (Rivard et al., 2011) and is now widely used (Feldman & Horan, 2011). Forecasts also predict a boom in the HIT market over the next several years (RNCOS, 2011a; RNCOS, 2011b; RNCOS, 2011c). Organizations using HIT can jeopardize the privacy of patients' PHI in many ways. HIPAA violations include actions as simple as improperly positioning computer monitors and more complex violations such as failing to encrypt patient data sent to doctors' mobile phones or failing to implement compliance policies and structures. Given the ubiquitous use of HIT, the U.S. Government passed an extension of HIPAA called the HITECH Act into law. The HITECH Act offers further direction about how to safely use HIT to improve the healthcare industry (HHS, 2011).

PCI DSS

PCI DSS is an industry standard established by a coalition of large credit card providers, such as Visa, to encourage organizations to proactively protect consumer credit card information from computer crackers. Private-sector organizations, not government agencies, govern PCI DSS (Morse & Raval, 2008). As such, PCI DSS offers few legal remedies. Instead, the private-sector organizations enforce PCI DSS by raising transaction charges, fining violators, revoking the right to process credit card transactions, and by requiring organizations to undergo audits and/or to hire qualified security assessors (Owen & Dixon, 2007; Rees, 2010). PCI DSS auditing requirements differ according to the number of transactions that an organization processes (Morse & Raval, 2008; Owen & Dixon, 2007). Major PCI DSS requirements include building a secure network with well-configured firewalls, encrypting credit card data, establishing strong virus controls, maintaining logs, conducting penetration testing, and devising appropriate security policies (Owen & Dixon, 2007).

SOX

SOX is U.S. federal legislation passed to increase accountability for accounting-related fraud and errors (Leon, Abraham, & Kalbers, 2010). SOX requires organizations to adopt internal controls and guidelines for financial reporting. For example, organizations must provide quarterly and annual reports to the Securities and Exchange Commission (Smith, 2003). Accounting practices are embedded in organizations' IT; therefore, designing accounting systems appropriately is required for SOX compliance (Smith, 2003; Mishra & Weistroffer, 2007). Mishra and Weistroffer (2007), for example, provide a framework for developing SOX-compliant software. SOX allows for criminal prosecutions of organizations and individuals involved in financial fraud. Nonetheless, no major penalties have been levied against an organization based on this legislation. The potential penalties for SOX noncompliance may include fines of up to USD$5 million or imprisonment for up to 20 years (CULS, 2012).

Appendix B: Potential Testing of SOIPSVM and Operationalizations of Its Constructs

A primary limitation of SOIPSVM is no study has empirically tested it yet—importantly, neither has anyone empirically tested SORVM. To facilitate researchers' in future testing SOIPSVM, we briefly address ways one might operationalize and test its constructs. In this appendix, we do not propose the optimal measurement of the constructs (one can measure most constructs in multiple ways); rather, we propose a first step in generating ideas for future research to test our model. Thus, using discretion is pivotal in selecting the most appropriate and representative measures to maximize construct validity. One could measure the relationships in SOIPSVM using a variety of research designs (e.g., field survey, secondary data). Here, we suggest some approaches for testing the model:

Survey of Multiple Organizations

First, one could test the model by developing a survey instrument to distribute to a sample of organizations. One could create measures for the survey through a development process similar to that proposed by MacKenzie, Podsakoff, and Podsakoff (2011) and Lewis, Templeton, and Byrd (2005), or one could adapt measures from existing research. Table B1 presents a list of measures that are potentially adaptable to the SOIPSVM context. As with the research design, one could use many existing scales for certain constructs. Researchers, therefore, should be thoughtful in selecting appropriate measures. For example, one might select existing measures for their psychometric properties or relation to the domain of interest. One could analyze survey results using PLS or SEM procedures. Although IS researchers use survey research frequently and successfully, it has limitations. For example, the results of the survey approach described above do not establish causal links between constructs. Instead, they offer support for the existence of the relationships. Establishing the temporal precedence of events is not possible in the survey method described above. Survey research also lacks the richness of insight that one can obtain through qualitative research.

Use of Experimental Scenarios

Second, preliminary studies could test the hypotheses through a scenario-based approach in which executives, preferably multiple executives from each organization, receive hypothetical vignettes to test the underlying theory. This approach is similar in design to a factorial experiment (and is, thus, termed the *factorial survey method*); different respondents receive different "treatments" in the scenarios. For example, some surveys would contain scenarios where centralization of power is high in the hypothetical organization. Other versions of the scenario would include a description of an organization where centralization of power is low. One applies this manipulation of the constructs to a subset of the constructs of the model. One would then ask participants to indicate what their perceptions of risk associated with a potential rule violation (using validated perceived risk survey measures—see Table B1) would be and what their perceptions of the likelihood that the organization would commit the violation would be if they were in power in the given organization. This approach has advantages for dealing with organizational rule violations that participants do not want to disclose their individual involvement in and knowledge of and has been effectively used in individual IS compliance research (e.g., Hu et al., 2011a; Siponen & Vance, 2010; Vance et al., 2015). Because the scenarios act as experimental groups, one can establish further evidence of causal links between constructs. However, this design also has disadvantages, including respondents' being unfamiliar with the situation and those who respond to the survey without real concern for the results. Some have also criticized scenario-based research because it may facilitate emotional detachment between the respondent and the scenario and, therefore, fail to capture participants' likely responses in real-world situations.

Field Studies

A third possibility for testing our model is to move toward more challenging field studies of actual organizations required to follow HIPAA or other IS security and privacy rules. More complex testing could also potentially use large samples of randomly selected organizations and randomly selected individuals in these organizations.

These field studies could involve organizational leaders responding to surveys; several survey measures exist for some of the constructs (see Table B1). However, some of these measures were developed for scenario-based studies, and one would need to adapt them to account for actual events. Other constructs (e.g., structural secrecy, violation coupling, and rule connectedness) are not closely associated with existing

survey measures, which makes operationalization more challenging. One would need to develop and validate new survey measures.

Another alternative for organizational field studies is to supplement survey measures with direct observation by and/or interaction involving researchers in the organizational setting. In this case, researchers would measure organizational characteristics in different ways depending on the construct. Researchers could examine hierarchies of the organization to determine centralization, monitor employee interaction to determine informal communication, and interview top organizational personnel to determine structural secrecy and violation coupling. To measure rule characteristics, the researchers would obtain a list of rules to which the organization is subject (e.g., HIPAA, PCI DSS, etc.) and then determine characteristics of the rules as perceived by the organization or as shown by its actions.

Secondary Data Analysis and Mixed Methods

One could also test the SOIPSVM model by using secondary data as operationalizations of the constructs. For example, the research team could collect news articles over a given time period that record violations of specific security and privacy rules. Researchers could determine, for example, the severity and celerity of punishments for rule violation for a given rule by aggregating news reports about such violations from several organizations. The researchers would then gather more information from the media or from violating organizations about relevant constructs that the news reports do not disclose. To supplement these data, it should be possible to use other secondary data (e.g., 10K reports) to clarify the structure of the organizations and other key constructs.

Finally, a mixed-methods approach is a useful alternative to keep in mind. Whereas one may best measure some constructs by survey, for example, one may best measure others by secondary data retrieval. A mixed-methods approach could compensate for the disadvantages of the individual research designs.

Table B1. Possible Survey Measures of SOIPSVM Constructs

Construct	Survey items	Notes
Formal communication structures: centralization (option A)	Our business transactions with other units should be approved by upper management.	Borrowed from Tsai (2002). Rated 1 to 7 (strongly disagree to strongly agree).
	Any agreement or dispute over inter-unit activities should be reported to upper management, and we should let management settle the issue.	
	Upper management has the ultimate power to decide whether we collaborate with other units in the organization.	
Formal communication structures: centralization (option B)	Extent to which decision making responsibility concerning capital budgeting is centralized at the highest levels of management.	These are directly replicated from (Lin, 2006, p. 431). They used a Likert-type scale from 1 = strongly disagree to 5 = strongly agree.
	Extent to which decision making responsibility concerning new product introduction is centralized at the highest levels of management.	
	Extent to which decision making responsibility regarding entry into major new markets is centralized at the highest levels of management.	
	Extent to which decision making responsibility regarding pricing of major product lines is centralized at the highest levels of management.	
Informal communication structures	Formal…informal	Kraut, Fish, Root, & Chalfonte (2002) proposed and studied these dimensions of informal communication in their observational organizational research. Could be used as a semantic differential scale.
	Scheduled in advance…unscheduled	
	Arranged participants…random participants	
	Participants in role...participants out of role	
	Preset agenda...unarranged agenda	
	One-way...interactive	
	Impoverished content...rich content	
	Formal language...informal language	

Table B1. Possible Survey Measures of SOIPSVM Constructs

Networking opportunities (possible insights into informal communication structures)	On average, how many days per year do you spend in interdepartmental committees, teams, and task forces?	Borrowed from Ghoshal et al. (1994).
	On average, how many days per year do you spend in interdepartmental meetings and conferences?	
	On average, how many days per year do you spend in meetings with upper management?	
Violation coupling	The positive external consequences of violating [specific rule or standard] are clear to key decision makers in this organization.	This concept is new to the literature and not directly based on a previous research stream; thus, it needs the most work. We propose these items based on the construct definition that Lehman & Ramanujam (2009) provide. We also believe it would be most effective to ground the concept in the particular violation context studied (e.g., HIPAA violations).
	The positive internal consequences of violating [specific rule or standard] are clear to key decision makers in this organization.	
	The negative external consequences of violating HIPAA are clear to key decision makers in this organization.	
	The negative internal consequences of violating [specific rule or standard] are clear to key decision makers in this organization.	
	If managers in my organization intentionally violated [specific rule or standard], specific, predictable outcomes (negative and/or positive) would occur.	
Certainty of sanctions	It is routine for Health and Human Services to audit our organization to identify HIPAA computer violations. [HIPAA as example].	Borrowed from Hu et al. (2011a). Rated 1 to 7 (strongly disagree to strongly agree).
	Organizations that violate [insert a particular IT rule here] will be caught.	
	It is likely that a violation of [insert a particular IT rule here] can be traced back to the violating organization.	
Severity of sanctions	Organizations caught violating [insert a particular IT rule here] will be severely punished.	Borrowed from Hu et al. (2011a). Rated 1 to 7 (strongly disagree to strongly agree).
	Organizations caught violating [insert a particular IT rule here] will be reprimanded.	
	Organizations caught violating [insert a particular IT rule here] will face serious consequences.	
Celerity of sanctions	For our organization, actions against violating [insert a particular IT rule here] are immediate.	Borrowed from Hu et al. (2011a). Rated 1 to 7 (strongly disagree to strongly agree).
	For our organization, actions against violating [insert a particular IT rule here] are instantaneous.	
	For our organization, actions against violating [insert a particular IT rule here] are timely.	
Goal clarity (in place of procedural emphasis)	It is clear what outcomes are expected in the rule that states [insert a particular IT rule here].	Borrowed from Tziner et al. (1993). Rated 1 to 7 (strongly disagree to strongly agree).
	The information provided on the [organization that administers a given privacy or security standard] website about [insert a particular IT rule here] will help you protect patients' medical information.	
	The information provided on the [organization that administers a given privacy or security standard] website about [insert a particular IT rule here] was sufficiently unambiguous.	
	The information provided to you by [organization that administers a given privacy or security standard] about [insert a particular IT rule here] was sufficiently detailed.	
Rule connectedness	[Specific IT rule] is highly connected to other rules with which our organization must comply.	Because no prior literature has

Table B1. Possible Survey Measures of SOIPSVM Constructs

	Complying with [specific IT rule] requires our organization to comply with other information security rules.	empirically tested rule connectedness, we propose these items as potential survey items to measure perceptions of rule connectedness (Lehman & Ramanujam, 2009; Sullivan, 2010). One measures these items on a Likert-like scale ranging from disagree to agree.
	By complying with [specific IT rule], our organization is automatically complying with many other rules.	
	A violation of [specific IT rule] would be problematic because it would entail a violation of other rules at the same time.	
Perceived risk of violations	What do you believe is the risk for your organization due to the possibility that: my organization could be issued severe sanctions for violations of [insert a particular IT rule here].	Borrowed from Dinev & Hart (2006). Rated 1 to 7 (very low risk to very high risk).
	What do you believe is the risk for your organization due to the possibility that: the media could damage my organization's image by sharing information about violations of [insert a particular IT rule here] committed by my organization.	
	What do you believe is the risk for your organization due to the possibility that: my organization will be caught if it violates [insert a particular IT rule here].	
Economic strain: performance relative to industry average	Determine the industry of an organization using the four-digit standard industry classification (SIC) code. Examine organizations' sales data using data from Compustat or an equivalent database for organizations with the SIC code of the focal organization. Compare the focal organizations' sales to the average sales of organizations with the same SIC code.	Borrowed from Harris & Bromiley (2007).
Noneconomic strain: conflict between rules and core values	[Insert a particular IT rule here] conflicts with the core values of my organization.	Newly developed. Rated 1 to 7 (strongly disagree to strongly agree).
	If my organization follows [insert a particular IT rule here], we will have to sacrifice some of the core values of my organization.	
	By following [insert a particular IT rule here], my organization will not be able to follow its core values.	
Likelihood of violation	If you were an employee at this organization, what is the likelihood that you would have violated [insert a particular IT rule here] [on behalf of your organization]?	Borrowed from D'Arcy et al. (2009). Rated 1 to 7 (very unlikely to very likely).
	I could see myself violating [insert a particular IT rule violation here] [on behalf of the organization] if I were in this situation.	

About the Authors

Jeffrey D. Wall is an Assistant Professor in the School of Business and Economics at Michigan Technological University. His research interests include individual and organizational deviance. His research examines information security and privacy behaviors of employees in organizations. He also studies organizational behaviors related to the use and misuse of information assets. His research has appeared in *Communications of the AIS*, the *Journal of Information Privacy and Security*, the *Journal of Global Information Technology Management*, and in the proceedings of several IS conferences**.**

Paul Benjamin Lowry is a Full Professor of Information Systems at the Department of Information Systems, City University of Hong Kong. He received his Ph.D. in Management Information Systems from the University of Arizona and an MBA from the Marriott School of Management. He has published 75+ journal articles in *MIS Quarterly, Information System Research, J. of Management Information Systems, J. of the AIS, Information Systems J., European J. of Information Systems, IJHCS, JASIST, I&M, CACM, DSS*, and many others. He is an SE at *Decision Sciences* and *AIS-Transactions on HCI*. He serves as an AE at *European Journal of IS, Information & Management, Communications of the AIS*, and the *Information Security Education Journal*. He has also served as an ICIS, ECIS, and PACIS track chair in various security/privacy tracks. His research interests include organizational and behavioral security/privacy issues; HCI and decision sciences; e-commerce and supply chains; and scientometrics.

Jordan B. Barlow is an assistant professor in the Information Systems & Decision Sciences department of the Mihaylo College of Business & Economics at California State University, Fullerton. His research interests include behavioral aspects of virtual collaboration/communication and IT security/compliance. He has published research in *MIS Quarterly*, *Communications of the AIS*, *Group Decision & Negotiation*, and *Computers & Security*.