Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2018 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-26-2018

The Role of Abusive Supervision and Interactional Justice in Employee Information Security Policy Noncompliance Intention

Bowen Guan
School of Economics & Management,Tongji University, guanbw@tongji.edu.cn

Carol Hsu
School of Economics & Management,Tongji University, carolhsu@tongji.edu.cn

Recommended Citation

Guan, Bowen and Hsu, Carol, "The Role of Abusive Supervision and Interactional Justice in Employee Information Security Policy Noncompliance Intention" (2018). *PACIS 2018 Proceedings*. 33.
https://aisel.aisnet.org/pacis2018/33

The Role of Abusive Supervision and Interactional Justice in Employee Information Security Policy Noncompliance Intention

Research-in-Progress

Bowen Guan
School of Economics & Management,
Tongji University
Shanghai, Siping Road 1239, China
guanbw@tongji.edu.cn

Carol Hsu
School of Economics & Management,
Tongji University
Shanghai, Siping Road 1239, China
carolhsu@tongji.edu.cn

Abstract

Employee information security noncompliance behaviors may ruin an organization's reputation; thus, much scholarly effort has been devoted to reducing deviating behaviors in organizations. We attempt to determine what motivations may contribute to the formation of an employees' noncompliance behavioral intentions. The proposed research model links the relationship between abusive supervision and policy noncompliance intention in an information security context. Drawing on organizational justice research, this work explores the role of abusive supervision in employees' noncompliance with information security policy from an interactional justice perspective and further proposes that the effect of interactional justice on noncompliance intention is moderated by the certainty and severity of sanctions based on general deterrence theory. We present a theoretical foundation for this investigation and an empirical design for exploring this research question. We also propose a plan for a research design and data collection, with results to be presented in the future.

Keywords: Abusive supervision, interactional justice, information security policy, employee noncompliance intention, general deterrence theory

Introduction

Information systems (IS) security issues are already of increasing concern to IS scholars and organizational managers. In particular, threats from organizational insiders have been gaining attention (Willison and Warkentin, 2013). Organizations have implemented a series of information security policies to address threats from employees or other organizational insiders, such as consultants or third-party contractors. Regardless, security policy violation behaviors from employees at work, such as data theft, password stealing, sabotage, leaking corporate materials or secrets, cyberbullying, and cyberloafing, are still one of the major concerns identified in many industry reports. Currently, an increasing number of organizations are becoming aware of the seriousness of such deviance behaviors and are attempting to develop a variety of formal and informal organizational controls to reduce or deter these noncompliance behaviors (D'Arcy et al., 2009; Hsu et al., 2012). Recent security breach incidents show that employee negligence and noncompliance often cost organizations millions of dollars in losses (Herath and Rao, 2009a, b). Failure to prevent deviance behaviors to some extent is due to employee noncompliance with organizational information security policies. Therefore, a question remains as to whether organizations or academics have also realized the importance of taking necessary and effective countermeasures to overcome the problem of employee security policy violation or noncompliance.

Many research efforts have been devoted to determining how to effectively reduce employee information security policy noncompliance and to understanding the facilitators that might influence employee security policy noncompliance or violation intention. The previous literature largely uses general deterrence theory (GDT) from a criminological perspective to consider the deployment of formal and informal sanctions to deter employees from the misuse of organizational resources or noncompliance with security policies (D'Arcy and Herath, 2011). However, the findings from research based on GDT-based factors, such as the certainty and severity of sanctions, were found to be mixed by Lowry et al. (2015), Willison and Warkentin (2013) and D’Arcy and Herath (2011). Some extant studies showed that both the severity and the certainty of formal sanctions had an effective influence on employee behavior (Straub and Nance, 1990; Siponen et al., 2007), but in other studies, only severity or certainty was significant (D’Arcy et al., 2009; Herath and Rao, 2009a, b). A study by D’Arcy et al. (2009) showed that the perceived severity, but not certainty, of formal sanctions was negatively associated with IS misuse intention. Conversely, Herath and Rao (2009a, b) found that the perceived certainty of detection, but not perceived severity of penalty, was positively associated with IS security policy compliance intention. Additional studies have found that neither the severity nor the certainty of formal or informal sanctions have a significant influence (Siponen and Vance, 2010; Hu et al., 2011). These inconsistent and even sometimes contradictory findings based on GDT in the IS context led IS scholars to add other theories to their theoretical model, such as neutralization theory and organizational justice theory. It seems that GDT alone cannot explain employees’ compliance with information security policies, which has led researchers to consider the motivations that cause employees to violate organizational security policies.

In some organizational behavioral science studies, abusive supervision has been linked with workplace deviance (Tepper et al., 2009; Detert et al., 2007; Duffy, Ganster and Pagon, 2002; Dupre et al., 2006; Tepper et al., 2008). Much of this work has regarded abusive supervision as the motive that leads to employee revenge and retaliatory behaviors due to unfavorable and unjust treatment. It is reasonable to assume that abusive supervision may translate into higher rates of theft, sabotage, psychological distress, and possibly organizational failure (Tepper, 2007). However, there appears to be little attention being paid to the relationship between abusive supervision and deviance behaviors in the IS context. Therefore, a research question to ask is whether abusive supervision can be the motivation behind an employee’s intention to commit security policy noncompliance behavior. More specifically, we conceptualize employee IS policy noncompliance as a form of common organizational deviance, and we argue, concerning the role of abusive supervision in IS security research, that an unexplored issue is how abusive supervision influences employees’ intention of noncompliance with security policies. Our study regards abusive supervision as a motive that can trigger employee security policy noncompliance and aims to determine how abusive supervision motivates violation or noncompliance deviance behaviors.

In this research, to explore the connection between abusive supervision and employee information security policy noncompliance intention, our theoretical foundation builds upon organizational justice theory and further identifies the antecedent which might lead to the perception of a particular organizational injustice. While our research review indicated that organizational justice theory has been applied to explore employees’ compliance with organizational policies (Lim, 2002; Willison and Warkentin, 2013; Willison et al., 2016), most studies have primarily focused on procedural justice as the main theoretical construct. Unlike these studies, we consider the role of interactional injustice, especially when caused by abusive supervision, and its impact on employees’ security policy noncompliance. We strive to shed new light on the role of abusive supervision and its impact on employee policy noncompliance behavioral intention for IS research relying on interactional justice. Our research proposes a theoretical model to investigate the relationship between abusive supervision and employee information security policy noncompliance intention and to provide a deeper understanding of employee motives from an interactional justice perspective. Further, given studies of employee security policy compliance or violation intention based on GDT, we align our theoretical notion with this line of research by considering potential deterrents in our theoretical model. The certainty and severity of sanctions as extrinsic motivators influence employee intentions of security policy compliance in organizations (Herath and Rao, 2009). We examine the moderating role of certainty and severity of sanctions on the relationship between interactional injustice and employee information security policy noncompliance intention to provide a more comprehensive understanding of the motivation mechanism.

Literature Review

Much of the behavioral IS security research has focused on the deterrence of employees' IS security policy compliance/noncompliance and abuse or misuse of IS resources (Warkentin and Willison, 2009). A review of theory-based empirical studies on compliance behavior in IS reveals that the research used GDT to offer a theoretical explanation. GDT suggests that people are less likely to engage in illegal or deviant behaviors when they perceive that sanctions are certain and severe. However, the existing deterrence studies yielded mixed results for both positive and negative employee security behaviors. For instance, D'Arcy and Devaraj (2012) found that the threat of formal sanctions has both direct and indirect effects on employee technology misuse intention. Research by D'Arcy et al. (2009) showed that IS misuse intention was strongly influenced by the perceived severity of sanctions but not by the perceived certainty of sanctions. Herath and Rao (2009a, b) discovered that the increased certainty of detection has an unexpected, significant positive influence on intention to comply with security policy, but punishment severity was negatively related to security policy compliance intention. Findings from Siponen and Vance (2010) provided a compelling explanation for security policy violations. They did not find formal and informal sanctions to be predictors of employee's intention to violate IS security policy. Hu et al. (2011) found the nonsignificant influence of employee perceived deterrence on the intention to commit policy violations with regard to information technology.

Given these mixed results, IS researchers have made some efforts to offer alternative theoretical explanations for user compliance/noncompliance with IS security policies. For example, Siponen and Vance considered neutralization theory as their theoretical foundation and claimed that their empirical results highlight neutralization as an important factor to consider with regard to developing and implementing organizational security policies and practices (Siponen and Vance, 2010). Further, special attention has been paid to the justice framework, which has been identified as a useful theoretical lens for understanding employees' compliance/noncompliance with organizational security-related policies. For example, Lim (2002) found that when employees perceive their employers to be fair in terms of distributive, procedural, and interactional standards, they are less likely to employ a neutralization technique through the metaphor of the ledger, and employees are less likely to engage in cyberloafing when they cannot legitimize the act through the metaphor of the ledger.

By reviewing the relevant literature, we found that studies based on organizational justice theory mostly considered procedural justice. However, in our research, we pay particular attention to interactional justice because it reflects the interpersonal dimension of fairness and individuals' experience of interactional injustice when organizational representatives fail to treat them with respect, honesty, propriety, and sensitivity to their personal needs or engage in other behaviors that fit the definition of abusive supervision (Tepper, 2000). Our study aims to understand how abusive supervision influences employee intention of security policy noncompliance. Therefore, it is suitable to apply interactional justice to explain the relationship between abusive supervision and employee information security policy noncompliance intention. In summary, in this research, we attempt to contribute to this emerging research by identifying abusive supervision as a possible motive and examining its impact on employee intention to commit security policy violation or to engage in noncompliance behavior. We will offer a more comprehensive understanding of how the perception of interactional justice is influenced within the context of employee information security policy noncompliance.

Theoretical Background

Abusive Supervision

Abusive supervision has generated considerable attention in organizational behavioral science research (Tepper, 2007; Tepper et al., 2017). Tepper (2000) defined abusive supervision as "subordinates' perceptions of the extent to which supervisors engage in the sustained display of hostile verbal and nonverbal behaviors, excluding physical contact." This phenomenon, as reported by Tepper et al. (2017), has been experienced by 13.6% of the U.S. workforce and mostly leads to a broad range of destructive outcomes and costs in terms of psychological distress, low level of work morale, and organizational deviance. Over the years, the extant literature has focused on explaining the direct and mediating effects linking abusive supervision through a rich set of theoretical perspectives, such as organizational justice, frustration aggression theory, and affective commitment (Mitchell and Ambrose, 2012; Tepper et al., 2008; Thau and Mitchell, 2010). Scholarly efforts have been devoted to associating abusive supervision with workplace deviance behaviors from the justice framework perspective in the field of organizational behavioral science. For instance, Tepper (2000) proposed that the degree to which supervisors engaged in abusive behavior would affect subordinates' perceptions of organizational justice, which in turn would affect decisions about quitting, job satisfaction, life satisfaction, organizational commitment, conflict between work and family life, and psychological distress. Furthermore, as Tepper et al. (2009) noted, in several studies of abusive supervision, researchers argued that victims may take revenge by performing retaliatory acts likely to go undetected or acts that may be observed. They found that abusive supervision is more strongly associated with subordinates' organization deviance and supervisor-directed deviance when subordinates' intention to quit is higher. Aryee et al. (2007) found that supervisors who themselves experienced interactional injustice were more abusive toward their subordinates. In considering these results in an organizational setting, we consider abusive supervision as a motive to trigger employee deviance behavior in the field of information security.

Organizational Justice Theory

In organizational behavioral studies of abusive supervision, as Tepper et al. (2000) indicated, it can be speculated that organizational justice plays a role in explaining the effects of abusive supervision (Tepper et al., 2000). Organizational justice has been applied to examine the fairness of the exchange processes and interactions in employment relationships, including those between employees and their employers. Previous research has identified three dimensions of perceived organizational justice: distributive, procedural and interactional justice. Colquitt et al. (2001) claimed that distributive justice is fostered when outcomes are consistent with implicit norms for allocation, while procedural justice concerns fairness in the processes used to determine the allocation of those outcomes. Interactional justice refers to the quality of interpersonal treatment (i.e., interpersonal sensitivity and explanations/social accounts) received by employees (Floger & Cropanzano, 1998).

Additionally, scholars have found that different types of justice will play different and important roles in understanding the quality of organizational social relationships. For instance, Masterson et al. (2000) found that procedural justice affected organization-referenced outcomes (e.g., organizational commitment, turnover intentions), whereas interactional justice affected supervisor referenced outcomes (e.g., supervisory organizational citizenship behaviors). More importantly, they proved that an interactional justice–outcome relationship was mediated by the quality of individuals' social exchange relationship with their supervisor (operationalized by the quality of leader–member exchange) (Masterson et al., 2000). In particular, extant studies have mostly considered procedural justice rather than interactional justice in IS research. In this research, we consider abusive supervision as a trigger for damage to the perceptions of interpersonal treatment, so we particularly focus on the role of interactional justice in explaining how abusive supervision influences employee information security policy noncompliance intention.

In the IS context, the literature that applies the organizational justice framework has found empirical evidence that employees are more likely to commit negative actions when they perceive organizational injustice. Lim (2002) developed a theoretical model based on organizational justice and neutralization theory and suggested that when employees perceived distributive, procedural and interactional justice, they were less likely to engage in cyberloafing. Willison et al. (2016) examined employee computer abuse intentions from the justice, deterrence and neutralization perspectives, and they used organizational injustice as their theoretical foundation to investigate such negative outcomes. Some authors use justice, while others use injustice in their theoretical model. In this paper, we will use injustice because we focus on employee information security police noncompliance, which is a negative reaction to perceptions of organizational injustice. Hence, our theoretical model will use interactional injustice, which means that people are treated with impoliteness, rudeness, and disrespect by authorities or third parties involved in executing procedures or determining outcomes.

General Deterrence Theory

General deterrence theory (GDT) has been most often applied in behavioral IS security research to predict user behaviors that will probably disrupt IS security or other IS security-related outcomes. The GDT posits that if an offender perceives that the certainty and severity of the sanctions associated with a crime are high, then he or she will be deterred from engaging in a criminal act (Straub, 1990). Some IS deterrence-based studies assessed the influence of formal and informal sanctions on computer abuse/misuse and IS security policy compliance/noncompliance behavior. Scholars have found that such security behavior can be effectively deterred with the existence of deterrent constructs (i.e., certainty of sanctions; severity of sanctions; and celerity of sanctions) (Herath and Rao (2009a, b); D'Arcy and Devaraj (2012); D'Arcy et al. (2009); Hu et al. (2011); Warkentin and Willison (2009)) Although the findings were mixed in IS research, evidence has been provided that the deterrent effect of the formal and informal sanctions was effective. In this paper, we also consider the moderating role of the severity and the certainty of sanctions; the celerity of sanctions was excluded in accord with the consensus which claims that sanctions celerity is difficult to measure and lacks theoretical importance (D'Arcy and Herath (2011)).

Hypothesis Developments

In the IS security context, some studies have conceptualized information security policy violation or employees' policy noncompliance from the organization deviance perspective. Lim specifically concentrated on the deviance act of cyberloafing and assigned this behavior to the category of production deviance (Lim, 2002), while Lowry et al. (2015) broadly used organization deviance to describe employee reactive computer abuse in response to enhanced information security policies. Here, we conceptualize such deviance behavior, which violates information security polices, when employees perceive their superiors' abuse as unjust treatment. To date, few studies have directly examined the relationship between abusive supervision and employee policy noncompliance intention. We consider abusive supervision and aggression towards subordinates as a trigger for perceived injustice and even retaliation behavior. As Tepper and Bennett (2000) noted, individuals experience interactional injustice when their superiors treat them with behaviors that fit the definition of abusive supervision. Consistent with this notion that subordinates should experience organizational injustice when their supervisors are more abusive (Tepper and Bennett, 2000), we hypothesize that,

H1: Abusive supervision is positively related to employee perceived interactional injustice.

Based on the organizational justice framework, we consider interactional injustice to be a strong predictor of abusive supervision triggering employees' intention to violate information security policies. The introduction and implementation of rules need a relative justice climate so that organizations can take effective measures to reduce and deter employees' noncompliance with information security policies. Several studies have already applied the justice framework as an under-researched area in understanding employees' compliance with security policies in the workplace (e.g., Lim, 2002; Lowry et al., 2015; Willison and Warkentin, 2013). For instance, Lim (2002) proposed that in the employment relationship, employees perform their job duties in return for some expected combination of economic and relational rewards from their employers. When employees perceive that their employers have not lived up to their end of the bargain, they will be motivated to reinstate justice in some way (Lim, 2002). In our research, we expect that when employees believe that interactional justice is unsatisfied because of their abusive supervisor, they will be more likely to retaliate against their employer by violating related rules. Thus, we hypothesize that,

H2: Perceived interactional injustice is positively related to employees' security policy noncompliance intention.

IS researchers have also noted the need to consider several extrinsic and intrinsic motivators that may encourage security policy compliance in organizations (Herath and Rao, 2009). Empirical studies on compliance with IS security policies and computer abuse suggest that formal sanctions can predict information security policy violations, but with mixed results. However, we involved the formal sanctions in our study as the moderating variables of the effect of interactional injustice on noncompliance intention. In considering the severity of punishment, the literature suggests that as the level of punishment increases, an individual becomes less likely to carry out a deviant act, and with higher awareness of existing detection mechanisms in the workplace, employees are more likely to comply with security policies (Herath and Rao, 2009a, b). We argue that the certainty of sanctions and the severity of sanctions may negatively moderate the relationship between perceived interactional injustice and employees' security policy noncompliance intention. Thus, we hypothesize that,

H3a: The greater the perceived certainty of sanction, the weaker the relationship between perceived interactional injustice and employees' security policy noncompliance intention.

H3b: The greater the perceived severity of sanction, the weaker the relationship between perceived interactional injustice and employees' security policy noncompliance intention.

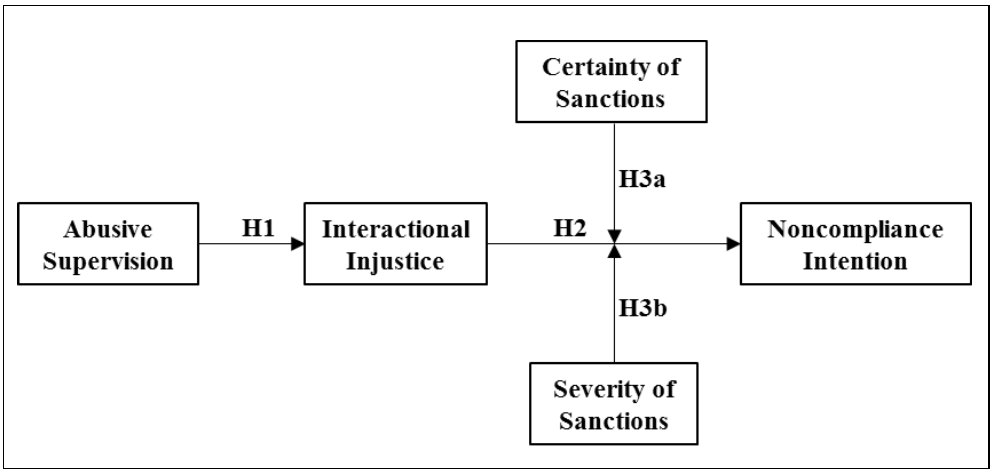

Figure 1. Theoretical Model Depicting the Role of Abusive Supervision and Information Security Policy Noncompliance Intention

Our theoretical model, shown as Figure 1, illustrates plausible motives that may influence employee security policy noncompliance intention. We expect that abusive supervision will be a trigger for the perceived interactional injustice of employees and that interactional injustice will act as a factor that affects employee information security policy noncompliance. In addition, the certainty and severity of sanctions are moderating variables that may negatively moderate the relationship between interactional injustice and employees' security policy noncompliance intention.

Research Design

In this paper, we plan to collect data from one online survey company. We require the company to select participants who are full-time employees and aware of their current organizational information security policy. Participants who consent will complete the questionnaire. The research company will send invitation emails to participants to create a diverse population. Respondents will be given points-based incentives for their participation.

The measurements of our research variables are adapted from previous research and revised according to our research context. All items are measured on a 5-point Likert scale from 1 to 5. The items of abusive supervision are adapted from Tepper (2000). Interactional justice is measured using items from Niehoff and Moorman (1993). IS security policy compliance intention items are adapted from Burcu Bulgurcu et al. (2010). The severity and certainty of sanctions are measured using items developed by Lowry et al. (2015).

We will conduct a pretest for a total of 100 responses. According to the pretest results, we will modify our questionnaire and then conduct our final survey. This paper plans to design a two-wave survey to empirically test the hypothesized research model. To investigate IS security policy compliance, we plan to separate the two steps by 3 weeks. At time 1, we expect the online survey company to send invitation emails to users about the study purpose and ask for their participation. Participants will be asked to answer questionnaires about their perception of abusive supervision, interactional justice and the certainty and severity of sanctions. Participants' unique user accounts can be used to trace the responses and match the survey at time 1 with the survey at time 2. At time 2, after three weeks, we expect to measure the employees' IS security policy compliance intention. Finally, participants will be asked to complete the questionnaire to capture control variables, including employee gender, age, tenure with the supervisor, organizational tenure, computer use, education level, income, organizational size, and negative affectivity (adapted from Lowry et.al. (2015)).

Expected Contribution

First, our empirical findings are expected to make a theoretical contribution by enhancing our understanding of the impact of abusive supervision on employees' security policy noncompliance intention. Although prior research has concentrated on the relationship between abusive supervision and various workplace deviance behaviors, very little is known about the impact of abusive supervision on employees' noncompliance intention. Second, our research from a justice framework perspective is expected to explain insider motives. While most previous studies based on organizational justice theory tend to adopt procedural justice, few considered interactional justice as a plausible factor. In addition, we add the certainty and severity of sanctions into our theoretical model, which will provide a more comprehensive understanding of the issue we discuss. More details will be researched and presented in the future.

References

Aryee, S., Chen, Z. X., Sun, L., and Debrah, Y. A. 2007. "Antecedents and Outcomes of Abusive Supervision: Test of a Trickle-Down Model," *Journal of Applied Psychology* (92), pp. 191–201.

Brian P. Niehoff and Robert H. Moorman. 1993. "Justice as a Mediator of the Relationship between Methods of Monitoring andOrganizational Citizenship Behavior," *Academy of Management Journal* (36:3), pp. 527-556.

Burcu Bulgurcu, Hasan Cavusoglu and Izak Benbasat. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefsand Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Colquitt, J., Conlon, D., Wesson, M.J., Porter, C. & Ng, K. 2001. "Justice at the millennium: a meta-analytic review of 25 years of organizational justice research, " *Journal of Applied Psychology* (86), pp. 425–445.

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

D'Arcy, J., and 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), pp. 643-658.

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

Detert, J. R., Trevino, L. K., Burris, E. R., and Andiappan, M. (2007). "Managerial Modes of Influence and Counterproductivity in Organizations: A Longitudinal Business Unit-Level Investigation, " *Journal of Applied Psychology* (92), pp. 993–1005.

Duffy, M. K., Ganster, D. C., and Pagon, M. 2002. "Social Undermining in the Workplace, " *Academy of Management Journal* (45), pp. 331–351.

Dupre, K. E., Inness, M., Connelly, C. E., Barling, J., and Hoption, C. 2006. "Workplace Aggression in Teenage Part-Time Employees," *Journal of Applied Psychology* (91), pp. 987–997.

Folger, R., and Cropanzano, R. 1998. *Organizational Justice and Human Resource Management*. Thousand Oaks, CA: Sage Publications.

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

Herath, T., and Rao, H. R. 2009b. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154-165.

Hsu, C., Lee, J.-N., and Straub, D. 2012. "Institutional Influences on Information Security Innovation," *Information Systems Research* (23:3), pp. 918-939.

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

Lim, V. 2002. "The It Way of Loafing on the Job: Cyberloafing, Neutralizing and Organizational Justice," *Journal of Organizational Behavior* (23:5), pp. 675-694.

Lowry, P., Posey, C., Bennett, R., and Roberts, T. 2015. "Leveraging Fairness and Reactance Theories to Deter Reactive Computer Abuse Following Enhanced Organizational Information Security Policies: An Empirical Study of the Influence of Counterfactual Reasoning and Organizational Trust," *Information Systems Journal* (25:3), pp. 193-203.

Mitchell, M., and Ambrose, M. 2012. "Employees' Behavioral Reactions to Supervisor Aggression: An Examination of Individual and Situational Factors," *Journal of Applied Psychology* (97:6), pp. 1148-1170.

Masterson, S. S., Lewis, K., Goldman, B. M., and Taylor, M. S. 2000. "Integrating Justice and Social Exchange: The Differing Effects of Fair Procedures and Treatment on Work Relationships," *Academy of Management Journal* (43), pp. 738–748.

Siponen, M., Pahnila, S., and Mahmood, A. 2007. "Employees' Adherence to Information Security Policies: An Empirical Study," in *Proceedings of the IFIP SEC 2007*, Sandton, Gauteng, South Africa, pp. 133-144.

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

Straub, D.W. and Nance, W.D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study, " *MIS Quarterly* (14), pp. 45–60.

Tepper, B. 2000. "Consequences of Abusive Supervision," *Academy of Management Journal* (43:2), pp. 178-190.

Tepper, B. 2007. "Abusive Supervision in Work Organizations: Review, Synthesis, and Research Agenda," *Journal of Management* (33:3), pp. 261-289.

Tepper, B., Henle, C., Lambert, L., Giacalone, R., and Duffy, M. 2008. "Abusive Supervision and Subordinates' Organization Deviance," *Journal of Applied Psychology* (93:4), pp. 721-732.

Tepper, B., Carr, J., Breaux, D., Geider, S., Hu, C., and Hua, W. 2009. "Abusive Supervision, Intentions to Quit, and Employees' Workplace Deviance: A Power/Dependence Analysis," *Organizational Behavior and Human Decision Processes* (109), pp. 156-167.

Tepper, B., Simon, L., and Park, H.-M. 2017. "Abusive Supervision," *Annual Review of Organizational Psychology and Organizational Behavior* (4), pp. 123-152.

Thau, S., and Mitchell, M. 2010. "Self-Gain or Self-Regulation Impairment? Tests of Competing Explanations of the Supervisor Abuse and Employee Deviance Relationship through Perceptions of Distributive Justice," *Journal of Applied Psychology* (95:6), pp. 1009-1031.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1-20.

Willison, R., Warkentin, M., and Johnston, A. 2016. "Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives," *Information Systems Journal* (in press), p. DOI: 10.1111/isj.12129.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat, " *European Journal of Information Systems* (18:2), pp. 101-105.