
Jeffrey Wall  
*Information Systems and Operations Management, University of North Carolina--Greensboro, Greensboro, NC, United States., jdwall2@uncg.edu*

Lakshmi Iyer  
*ISOM, The University of North Carolina at Greensboro, Greensboro, NC, United States., Lsiyer@uncg.edu*

Follow this and additional works at: [http://aisel.aisnet.org/amcis2012](http://aisel.aisnet.org/amcis2012)

Recommended Citation  
[http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/12](http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/12)

Jeffrey D. Wall
University of North Carolina at Greensboro
jdwall2@uncg.edu

Lakshmi S. Iyer
University of North Carolina at Greensboro
Lsiyer@uncg.edu

ABSTRACT

This paper presents a conceptual model to explain employee security behaviors as a function of manager’s transgressions in the workplace. To date, most information systems security (ISS) studies neglect the effects poor leadership can have on the security of organizational ISS. This paper seeks to broaden the study of leadership in information systems security by examining negative effects of leadership. This paper suggests that leader transgressions create punitive desires in employees that result in ISS-related deviance. This paper identifies two forms of deviance, intentional policy non-compliance and less intentional neglect of proactive security behaviors. Importantly, although other studies mention these two forms of deviance, this paper is one of few that model them together. The model in this paper can help leaders understand the effects of their negative behaviors and direct leaders toward ways to improve relationships with employees, and thereby enhance security.

Keywords

Information systems security, leadership, transgression, justice, injustice, non-compliance employee deviance behavior

INTRODUCTION

Information Technology (IT) Security breaches or the threat thereof can negatively affect organizational profits and innovation. The Computer Security Institute (CSI) reports, for example, that the average annual loss to organizations due to security-related problems was nearly $290,000 in 2008 and $235,000 in 2009 (Richardson, 2009). Similarly, CSI reports that security spending is on the rise; security spending rose from 12.8% of an organization’s IT budget in 2009 to 18.6% in 2010 (Richardson, 2011). Several e-government studies identify security-related issues as a major barrier to the furtherance of e-government initiatives such as e-voting (McClure, 2001; Moon, 2002; West, 2004). Clearly, creating secure information systems (IS) is a costly endeavor, and if not done well, may impede the progress of IS-related initiatives or cause undue cost to organizations.

Recent information systems security (ISS) studies point to organizational insiders as a major threat to information security and privacy in organizations (Warkentin & Willison, 2009; Workman & Gathegi, 2007), but also suggest that organizational insiders can be a great security asset (Bulgurcu, Cavusoglu, & Benbasat, 2010). These studies tend to focus on employees’ intentions to comply with IT security policies or security behaviors (Bulgurcu, et al., 2010; Herath & Rao, 2009; Puhakainen & Siponen, 2010; Warkentin, Johnston, & Shrophire, 2011), or employees’ intentions to violate IT security policies or misuse IT resources (D’Arcy, Hovav, & Galletta, 2009; Siponen & Vance, 2010; Straub, 1990). Other security studies focus on outcomes such as employee precaution taking (Boss, Kirsch, Aungermeier, Shingler, & Boss, 2009; Png & Wang, 2009) and employee negligence (Workman, Bommer, & Straub, 2008).

Most ISS studies explicitly or implicitly assume that employees are organizational threats, and organizational leaders are benevolent actors that can minimize employee threats or transform employees into security assets. Few IS security studies, however, examine the assumption of leaders’ benevolence. In a review of ISS research, Zafar and Clark (2009) suggest leadership is an important facet of ISS governance that needs to be examined further. Research is only beginning to question the effect leaders’ negative actions can have on employee security behaviors. Leach (2003), for example, suggests that the violation of ISS-specific psychological contracts by managers may lead to deviant security-related behaviors by employees. He does not, however, test these assertions. Similarly, Posey, Bennett, Roberts, and Lowry (2011) suggest that employees’ perceptions of workplace injustice related to computer monitoring can increase intentions to misuse organizational IT. They find that employees are more likely to engage in deviant IS behaviors if they believe managers’ computer monitoring behaviors are inequitable or that monitoring is an invasion of privacy.
The findings of Posey et al. (2011) are consistent with organizational literature on justice and injustice in the workplace. Aquino, Tripp, and Bies (2006), for example, show that employees’ reactions to managers’ interpersonal transgressions may result in revenge seeking. This paper seeks to further merge ISS research with research on workplace justice and injustice to examine the effects poor leadership can have on employee security behaviors. This paper addresses the following research question: how do leaders’ interpersonal transgressions at work affect employees’ intentions to violate information security policies or neglect information security behaviors? The model in this paper relies on studies of workplace injustice to show how leader transgressions may create punitive desires in employees that lead to deviant behaviors (e.g., Aquino, et al., 2006; Shapiro, Boss, Salas, Tangirala, & Von Glinow, 2011).

This paper offers three important contributions to ISS research and practice. First, this paper considers the antecedents of deviant behavior in employees seeking to punish transgressing leaders. Little has been done to consider these antecedents. Second, this paper considers both direct non-compliance and neglect in the same model. Although other ISS studies have mentioned the existence of these two separate forms of deviance, to our knowledge, no paper has attempted to model them together. Lastly, this paper can inform leaders’ behaviors. The model in this paper helps to inform leaders of the potential effects of their actions can have on employee deviance. Similarly, the model and related literature suggests ways that leaders can minimize punitive desires, and thereby, minimize employee deviance.

The remainder of this paper continues as follows. First, this paper presents a conceptual model based on previous literature to explain and predict the effects of manager transgressions on employee intentions to violate ISS policies and neglect security behaviors. Next, this paper discusses the implications of the model and offers directions for future research on leadership and ISS.

BACKGROUND AND CONCEPTUAL MODEL

ISS studies have mostly ignored the impact of leader transgressions on employee security behaviors. This paper attempts to bridge this gap by adopting studies of workplace injustice (e.g., Aquino, et al., 2006; Shapiro, et al., 2011) to explain and predict employee security violations. The model in this paper is called the Leader Transgression Model of Employee Information Security Deviance (LTMEISD). For the purpose of this paper, manager transgressions refer to any deviant act (e.g., mistreating an employee, violating company policies, arriving late to work) committed by managers that invokes feelings of disappointment, anger, or unfairness in employees. Punitive desires refer to an individual’s desire to see a transgressor harmed or brought to justice (Shapiro, et al., 2011).

Research on workplace injustice suggests that employees react to leader’s transgressions in different ways (Aquino, et al., 2006). Many studies on workplace injustice suggest that employees seek revenge and retaliation against injustice (e.g., Ambrose, Seabright, & Schminke, 2002; Aquino, Tripp, & Bies, 2001; Jones, 2009). Other studies, however, focus more on forgiveness and reconciliation (Aquino, et al., 2006; Shapiro, et al., 2011). Importantly, not all transgressions are met by revenge seeking (Aquino, et al., 2006). Individuals’ characteristics, leaders’ characteristics, leader-employee relationships and other environmental factors may make forgiveness more likely at times (McCullough & Hoyt, 2002; McCullough et al., 1998; Shapiro, et al., 2011). When employees do seek revenge for injustice, however, the retaliation may be toward the leader, the organization, or both (Jones, 2009). Employees, for example, are more likely to engage in IS-related deviance when they feel that their organizations’ computer monitoring behaviors are unfair or inequitable (Posey, et al., 2011). This paper uses the research mentioned above to examine factors that may lead employees to violate security rules and engage in insecure behaviors in retaliation to leader transgressions. Figure 1 depicts the entire research model.

Leader Transgressions and Punitive Desires

This paper argues that the quality of the working relationship between a transgressing leader and an employee will affect the employee’s desire to punish the leader. Studies on forgiving in interpersonal relationships show that individuals in satisfying relationships are less likely to seek revenge for a partner’s interpersonal transgressions (e.g., McCullough, et al., 1998). Shapiro et al. (2011) empirically demonstrate that the strength of an employee’s desire to punitively judge a transgressing leader is based upon the quality of the working relationship between the leader and employee. They suggest that idiosyncrasy credit theory (ICT) (Hollander, 1958) offers an explanation for their empirical findings. ICT posits that leaders emerge by displaying competence and conformity with group norms. ICT further suggests that displays of competency and conformity build idiosyncratic “credit” for the emergent leader that allows the leader to act in idiosyncratic ways without being judged by employees.

Research on transgressions in social relationships adds insight into the motivations that lead employees to forgive idiosyncrasies in leaders with high “credit” (e.g., McCullough, et al., 1998). Studies of interpersonal transgressions suggest that transgressions elicit reactive motivations in individuals, commonly termed as transgression-related interpersonal
motivations (TRIMs). Three TRIMs that predict an individual’s willingness to forgive a transgressor include: the TRIMs to avoid and seek revenge against the transgressor and the TRIM to be benevolent toward the transgressor (McCullough & Hoyt, 2002). Forgiveness occurs to the extent that an individual is willing to set aside TRIMs to avoid and seek revenge and feel a high TRIM to be benevolent toward the transgressor (McClore, 2001; McCullough, et al., 1998; McCullough, Worthington, & Rachal, 1997). When TRIMs to avoid and seek revenge are high and the TRIM to be benevolent is low, forgiveness is less likely and instead, individuals may desire to punish the transgressor (Hoyt, Finchman, McCullough, Maio, & J, 2005). When a transgressing leader has high “credit,” an employee is likely to have lower TRIMs to avoid and seek revenge and a higher TRIM to be benevolent toward the leader (Shapiro, et al., 2011).

Shapiro et al. (2011) suggest that leader-member exchange (LMX) is a useful representation of a leader’s idiosyncratic “credit,” as no measure for idiosyncratic “credit” currently exists (Stone & Cooper, 2009). LMX is a measure of the trust, respect, and loyalty an employee feels toward a leader (Graen & Uhl-Bien, 1995). LMX theory is closely related to and derived from ICT (Stone & Cooper, 2009), therefore, the LMX measure may be especially fitting as a measure of leader “credit.” Importantly, Shapiro et al. (2011) show that an employee is less likely to forgive idiosyncrasies in leaders with low LMX. Employees’ evaluations of LMX are likely to be higher to the extent that they believe leaders possess favorable traits (Diener & Liden, 1986; Howell & Hall-Merenda, 1999). Thus:

**Proposition 1:** A transgressing leader’s LMX has a negative relationship with an employee’s desire to punish the leader.

Beyond the quality of leader-employee relationships, research on organizational injustice shows that the relative hierarchical status of the transgressor affects the likelihood that the victim will seek revenge (Aquino, et al., 2001). Individuals are less likely to punish those perceived to hold greater relative power than they are to punish those perceived to have equal or less relative power (Kim, Smith, & Brigham, 1998). Punishment directed toward high status, transgressing individuals may result in retaliation from the transgressor (Heider, 1958). Importantly, higher status leaders have greater power over employees’ well-being. The hierarchical status of a leader determines the leader’s ability to determine the employee’s continuing status with the company, pay raises, promotions, etc. For example, a shift supervisor may have power to supervise an employee’s performance, but may have little or no power in determining whether an employee is fired. Employees may be willing to forgo retribution against high status leaders to avoid negatively affecting their standing with their organization (Aquino, et al., 2001). These findings are consistent with general deterrence theory (GDT) (Blumstein, 1978), which suggests that individuals will be less likely to engage in questionable behavior to the extent that sanctions for misbehavior are certain and severe. The premises of GDT are used extensively in ISS research to show how sanctions can deter negative security behaviors (e.g., D’Arcy, et al., 2009; Straub, 1990). This paper therefore proposes:

**Proposition 2:** An employee’s perception of the certainty that a transgressing leader will retaliate has a negative relationship with the employee’s desire to punish the leader.

**Proposition 3:** An employee’s perception of the severity of a transgressing leader’s retaliation has a negative relationship with the employee’s desire to punish the leader.

To this point, we have suggested that employees may be likely to forgo vengeful desires toward leaders out of respect or fear. We now argue, however, that an employee’s perception of the severity of a leader transgression will strengthen the employee’s desire to punish the leader. Severe offenses tend to elicit greater retribution than minor offenses (Miller & Vidmar, 1981). Although offense severity is rarely addressed as a primary construct in studies of workplace injustice, it is regularly used as a control variable (e.g., Aquino, et al., 2001; Aquino, et al., 2006; Shapiro, et al., 2011). Aquino et al. (2001, 2006), for example, show that offense severity is negatively related to reconciliation. Similarly, Shapiro et al. (2011) show that offense severity is positively related to an employee’s punitive desires. This paper submits that perceptions of severity may be affected by workplace norms. Employees’ perceptions of appropriate workplace behaviors are shaped by the behaviors and attitudes of important and respected members of the organization (Markham & McKee, 1995). Employees tend to follow the norms organizational authorities intentionally or unintentionally reward (Mayer, Chan, Hodges, & Avolio, 2009). If a leader’s transgression falls within the bounds of appropriate organizational behavior, then employees may not see the transgression as worthy of punishment (Shapiro, et al., 2011). This conclusion is supported by the finding that employees tend to mimic even antisocial normative behaviors (Robinson & O’Leary-Kelly, 1998). Given this discussion, this paper offers the following proposition:

**Proposition 4:** An employee’s perception of the severity of a leader transgression has a positive relationship with the employee’s desire to punish the leader.
Although the severity of a transgression has been shown to affect punitive desires, employees’ attributions of blame are the most powerful predictors of revenge seeking behavior (Aquino, et al., 2001, 2006). Attribution of blame refers to the extent to which an individual holds a transgressor accountable for the offense (Aquino, et al., 2001). Again, organizational norms may affect attributions of blame by shaping an individual’s perceptions of what is appropriate or inappropriate. Similarly, individual factors might also affect attributions of blame. Disagreeable employees or those with high negative affectivity, for example, are more likely to seek revenge against a transgressor (Skarlicki, Folger, & Tesluk, 1999). If a victim assigns blame to a transgressor, the victim is likely to experience anger (Aquino, et al., 2001), which increase the likelihood of punitive desires (Allred, 1999; Martinko & Zellars, 1998). Thus:

Proposition 5: An employee’s attribution of blame to a leader’s transgression has a positive relationship with the employee’s desire to punish the leader.

Punitive Desires and Employee Security Deviance

This paper posits that an employee’s punitive desires will increase the employee’s intention to violate information security policies (ISPs) and to neglect security-related precaution taking behaviors. Employees’ punitive desires may also increase their intentions to engage in other forms of abuse (e.g., Aquino, et al., 2001; Aquino, et al., 2006; Shapiro, et al., 2011), such as stealing office supplies, or physical and verbal abuse. However, these abuses are outside the scope of this paper. As discussed above, employee’s punitive desires toward a transgressing leader are affected by the leader-employee relationship, the perceived certainty and severity of a leader’s retaliation to punishment, perceptions of the severity of the transgression, and attributions of blame. Employees do not typically have the organizational power to directly punish a leader. Therefore, when punitive desires are high, employees may seek to punish the leader indirectly by engaging in deviant acts against the leader or the organization (Shapiro, et al., 2011). Importantly, leaders are often viewed as representing the organization (Eisenberger, Stinglhamber, Vandenbergh, Sucharski, & Rhoades, 2002). Employees may, therefore, harm the organization in retaliation to a leader’s transgression (Skarlicki & Folger, 1997).

This paper argues that certain circumstances may act to catalyze transgression spawned ISS-related deviance in employees. For example, transgressing IT managers or chief information officers (CIOs) may be more likely to invoke ISS deviance than line managers or chief executive officers (CEOs). This assertion is consistent with findings that retaliation is generally directed toward the cause of the injustice (Fox & Spector, 1999, 2006). This paper posits that employees will see ISS deviance as a direct punishment toward IT-leaders. Following this same reasoning, if a transgressing leader is a strong proponent of ISS then punitive desires are more likely to equate to ISS deviance. However, when employees feel unable to directly right a social wrong, they may engage in deviant behaviors unrelated to the offense (Bennett, 1998; Greenberger & Strasser, 1986). Employees, therefore, may engage in ISS-related deviance even when a transgressor has no direct connection to organizational security. This paper posits that intentional ISS-related deviance results from TRIMs to seek revenge. This assertion is consistent with the literature previously examined. Given this discussion, we propose the following proposition:

Proposition 6: An employee’s desire to punish a transgressing leader has a positive relationship with the employee’s intention to violate the organization’s information security policy.

Shapiro et al. (2011) show empirically that employees’ punitive desires toward a transgressing leader lead to psychological withdrawal from work. This assertion is supported by the work of Tyler and Blader (2000) who demonstrate that employees who negatively evaluate their leaders have less engagement and commitment to the organization. Psychological withdrawal behaviors include, but are not limited to employees: leaving work early, calling in sick when they are well, showing less effort in their work, using work time to accomplish personal tasks, and thinking about quitting their jobs (Lehman & Simpson, 1992). Given that punitive desires are partially formed by a TRIM to avoid the transgressor (McCullough, et al., 1998), which may be considered the organization (Skarlicki & Folger, 1997), it is not surprising that psychological withdrawal may result. Shapiro et al. (2011) suggest that employees may be particularly likely to engage in psychological withdrawal when they feel unable to directly punish a transgressing leader. Based on the work of Shapiro et al. (2011), this paper suggests:

Proposition 7: An increase in an employee’s desire to punish a transgressing leader will increase the employee’s psychological withdrawal from work.

Importantly, this paper argues that psychological withdrawal will lead to IT security negligence. Boss et al. (2009) suggest that IT security behaviors involve taking security precautions as prescribed by the ISPs, and additionally, engaging in proactive security behaviors that may not be prescribed in ISPs. Some proactive behaviors may include: considering security

issues during one’s daily routine, staying up-to-date with possible security threats, and making sure that one’s computer system remains as secure as possible. This paper views proactive behaviors as more goal oriented, while compliance to ISPs tend to be more procedural in nature. In this paper, IT negligence refers to neglecting these goal oriented, proactive behaviors that may not be part of the ISP. Since psychological withdrawal signifies a withdrawing from proactive behaviors, such as putting less effort into work, this paper submits that employees who withdraw from work will also withdraw from proactive security behaviors. In fact, since engaging in proactive security behaviors is not a primary work function for many employees, withdrawal from proactive security behaviors may be more likely than withdrawal from other work behaviors. Indirect evidence of computer-related withdrawal can be seen in the work of Lim (2002) and Lim and Teo (2005) who show that employees who feel they have been treated unfairly are more likely to engage in cyberloafing. Hence, the following proposition:

**Proposition 8:** An increase in an employee’s psychological withdrawal from work will increase the employee’s information security negligence.

**DISCUSSION AND IMPLICATIONS**

This paper has presented a conceptual model to explain employee security behaviors as a function of leader’s personal transgressions against employees. This paper has suggested that a leader’s transgressions may elicit from employees, desires to punish the leader. This paper has identified a series of factors that strengthen or weaken this desire to punish the transgressor. The quality of the relationship between the transgressing leader and an employee has a negative relationship with the employee’s desire to punish the leader. Similarly, an employee’s perception of the certainty and severity of backlash for punishing a transgressing leader has a negative relationship with the desire to punish. An employee’s attributions of blame and perceptions of the severity of the transgression may increase desires to punish the transgressing leader.

LTMEISD adds value to ISS research by examining the dark side of leadership in organizational IT security. This paper suggests that leadership is not always positive, a topic that is understudied in ISS research. Further, this paper expands on studies such as Posey et al. (2011) by making justice research a primary focus. Although Posey et al. (2011) examine theories of workplace justice, they take a very high level view. This paper contributes to work on justice theory in an ISS research by suggesting antecedents to justice-related deviance. This paper also identifies two distinct outcomes of punishment. The first, similar to the outcomes suggested by Posey et al. (2011), is deliberate violation of organizational policy or misuse of
organizational IT. The second, which has not been studied in justice-related research, is negligence of proactive security behaviors.

LTMEISD also offers insight into how transgressions should be handled in the workplace. For example, leaders should continually establish good rapport with employees by developing high LMX so that less major transgressions are not met by strong punitive desires that result in antisocial behavior. However, as Shapiro et al. (2011) point out, leaders set organizational norms. Norms set by well-respected leaders may also establish antisocial work behaviors. Therefore, it is important for leaders to continually monitor their behavior in order to set positive norms. Apologizing has also been identified as an important deterrent to revenge seeking behavior (Aquino, et al., 2006). Leaders should seek to establish just rules, enforce them fairly, and make necessary reconciliations when they violate employee expectations.

**Future Research**

Future research needs to test the assertions made in this paper. Many established measures exist to test the various propositions proposed in LTMEISD. For example, LMX measures can be borrowed from Graen and Uhl-Bien (1995). Certainty and severity of leader retaliation could be measured by adapting items from D’Arcy et al. (2009). And measures for employees’ desires to punish leaders could be borrowed from the work of Shapiro et al. (2011). Future research needs to continue to address the importance of leadership in ISS. Although much has been done to explain how leaders can prompt positive security behaviors, more work needs to be done to consider the antisocial effects of poor leadership.

**Conclusion**

Leaders play an important role in establishing secure information systems in organizations. However, leaders’ behaviors can also lead to antisocial behaviors in employees. Leaders must continually monitor their behaviors and quickly restore justice in the workplace to avoid employee retaliation. Research must continue to assess the important role of leaders in ISS.

**REFERENCES**


