Understanding Internet Abuses at Work Using Extended Rational Choice Theory

Research-in-Progress

Han Li
Minnesota State University
Moorhead
li@mnstate.edu

Xin Luo
University of New Mexico
luo@mgt.unm.edu

Jie Zhang
Midwestern State University
jie.zhang@mwsu.edu

Rathindra Sarathy
Oklahoma State University
rathin.sarathy@okstate.edu

Abstract

Employees’ violation of Internet use policy exposes firms to increasing security risks from cyber-attacks. Extant studies on security policy compliance have largely ignored the role of dispositional and contextual factors in employees’ decision. Drawing on the literature in criminology, this paper extended the rational choice theory by integrating low self-control and two organizational context factors to have a fine-grained understanding of the decision making process involved in Internet use policy compliance. The results will help indicate whether employees’ compliance intention is influenced by the cost-benefit calculus adjusted by their low self-control disposition, procedural justice perception and organizational moral climate. Research results are expected to be presented at the conference.

Keywords

Internet use policy, rational choice, low self-control, justice, moral climate.

Introduction

Internal employees may abuse the Internet access at the workplace to perform various non-work-related activities such as checking personal e-mails, browsing social network or other non-work-related Web sites, gaming, or watching streaming videos. To combat employee Internet abuse, the majority of companies have implemented Internet use policy (IUP) as one important type of security policies (CareerBuilder 2012; Clearswift 2007). Despite the wide deployment of IUP in companies, the scope of Internet abuse is still on the rise (Palo Alto Networks 2012). Violations of IUP are a top concern of information security management as over fifty percent of companies have fired workers for email and Internet abuse (Gohring 2008).

The poor compliance of IS security policies including IUP has piqued growing research interests in IS community. A large body of research has examined the information systems misuse as a result of rational decision involving the assessment of a variety of costs and/or benefits (Bulgureu 2010; D'Arcy et al. 2009; Hu et al. 2011; Li et al. 2010; Pahnila et al. 2007; Straub and Nance 1990). Despite the fruitful results from this body of research, far less research attention has been paid to the role of stable personal traits and organizational context factors in employees’ decision process. One’s stable personal trait to commit offensive acts such as low self-control, may interplay with the rational decision process (Hu et al. 2011; Nagin and Paternoster 1993). Besides stable personal traits, organizational context factors such as justice and moral climate against Internet abuses may influence employees’ motivation and their rational thought processes to perform deviant acts.
In an effort to fill the research gap, we further extended the rational choice perspective by incorporating the stable low self-control personal trait, procedural justice and organizational moral climate against Internet abuses. In particular, our research questions center on 1) how does low self-control influence employees’ decision process to comply with IUP? 2) how do procedural justice and organizational moral climate adjust the cost-benefit assessment of Internet abuses and their following intention to comply with IUP? 3) what are the mechanisms beyond traditional deterrence approach that facilitate IUP compliance?

Theoretical Foundation and Research Model

Prior studies have provided valuable insights into the compliance of security policies. However, they have generally ignored the effect of stable personal traits and organizational contexts in which non-compliance occurs. Moreover, different mechanisms enforcing security policy compliance were mostly examined independently from each other even if they are contrasted in the same model. There is a lack of fine-grained examination of the interplay among constructs of different theoretical perspectives. For example, it is not clear whether the effect of deterrence or the risk of violating security policies may be constrained by organizational contexts such as moral climate.

In this study, we proposed a research model (Figure 1) that integrates the rational choice framework with low self-control propensity and organizational context factors. Our research model provides a comprehensive understanding of corporate deviant behaviors by treating employees’ decision to comply with security policies as the results of cost-benefit tradeoffs interplayed with their personal trait, organizational justice and organizational moral climate. We do not simply compare them as independent competing forces driving IUP compliance. Instead, we provide a close examination of the interplays among these constructs from different theoretical perspectives, which may help us resolve inconsistency in findings of prior studies. In the subsections below, we first follow rational choice theory to discuss the effect of deterrence and perceived benefits of performing Internet abuses. Then, we elaborate the role of low self-control, procedural justice and organizational moral climate against Internet abuses in the rational choice framework.

![Figure 1. Research model. Positive effect \(\rightarrow\), negative effect \(\leftarrow\).](image)

IUP Compliance and Rational Choice Theory

Rational choice theory has been widely applied to explain deviant behaviors in many contexts. The theory has two basic premises: “(1) that decisions to offend are based on a balancing of both the costs and benefits of offending and (2) that what are important are the decision maker’s perceived or subjective expectations reward and cost” (Paternoster and Simpson 1996, p. 553). The first premise suggests that individuals weigh the costs and benefits of alternative courses of action and choose the one with the best
outcome. Employees are likely to violate security policies if the risks such as those from deterrence can be justified by the perceived benefits of deviant acts. Deterrence serves as “disincentives” weighed into individuals’ calculative assessment of the expected utility of a deviant act. It is expected to reduce the expected utility and make deviant acts less desirable. Therefore,

**H₂**: Deterrence has a positive impact on IUP compliance intention.

Sufficient benefits from rule breaking are anticipated for potential offenders to be willing to undertake the risks of deterrence. In the context of IUP compliance, the benefits could involve a more interesting work life from personal Internet usage, convenience or savings in cost and time over using private Internet access (Pee et al. 2008). These perceived benefits serve as situational enticements motivating employees to abuse the Internet access at their workplace, reducing their intention to comply with IUP. Therefore,

**H₂**: Perceived benefits of Internet abuses have a negative impact on IUP compliance intention.

**IUP Compliance and Low Self-Control**

The second premise of rational choice theory emphasizes that deviant behaviors result from subjective assessment of rewards and costs by individuals. The subjective nature of such assessment provides the basis for us to integrate low self-control in general crime theory (Gottfredson and Hirschi 1990) and rational choice theory closely to have a more comprehensive understanding of employee’s decisions to violate IUP. Low self-control is one type of criminal predisposition established early in life and remaining stable over one’s life (Gottfredson and Hirschi 1990). According to Gottfredson and Hirschi (1990), those lacking self-control tend to predispose them toward committing deviant and high-risk acts. In the context of our study, employees with low self-control may impulsively abuse the Internet access at the workplace for personal usage because they cannot wait to delay the usage until they go home. Also, the excitement and thrill from personal Internet activities at the workplace may help satisfy the risk-seeking property of those with low self-control. Therefore,

**H₃**: Low self-control has a negative impact on IUP compliance intention.

Individuals who are low in self-control are suggested to be unresponsive to sanctions but more responsive to tangible stimuli in the immediate environment and more enticed by short-term gratification (Gottfredson and Hirschi 1990; Grasmick et al. 1993). In addition, their risk-seeking tendency may also make them pay less attention to potential sanctions and be more disposed to deviant acts. Individuals with low self-control have been found to perceive more pleasure in deviant acts (Nagin and Paternoster 1993; Piquero and Tibbetts 1996) and higher benefits in violating IS security policies (Hu et al. 2011). Therefore, we argue that low self-control may also indirectly influence IUP intention by changing employees’ assessment of benefits of Internet misuses for personal purposes. Employees with strong low self-control propensity are expected to perceive Internet misuses to be more beneficial. Thus,

**H₄**: Low self-control has a positive impact on perceived benefits of Internet abuses.

Besides increasing perceived benefits of Internet abuses, low self-control may also moderate the effect of perceived benefits. For those with relatively strong low self-control, their impulsive tendency may become a more important driver for their performing Internet abuses, i.e. downplaying or even overriding the effect of perceived benefits. In this case, perceived benefits may only exert some trivial effect on IUP compliance intention. On the other hand, for those with weak low self-control, they are less impulsive and less risk-seeking. As a result, they are less driven by impulsivity. Their cognitive assessment of the benefits tends to become more prominent in shaping their decisions. Therefore, we hypothesize:

**H₅**: The relationship between perceived benefits of Internet abuses and IUP compliance intention is moderated by low self-control, such that the negative impact is stronger for those with weak low self-control.

**IUP Compliance and Organizational Context Factors**

Internet abuses in the workplace occur in specific organizational contexts. Until now, only a few studies on computer security and abuses examined the organizational context in which deviant behaviors occur. For example, Chan et al. (2005) found that a strong perception of the organizational security climate helps to curb non-compliant behaviors. Lim (2002) focused on organizational justice, suggesting that
perceived injustice in the employment relationship will cause employees to rationalize their subsequent engagement in Internet abuses.

In this study, we considered two organizational context factors that may indirectly or directly influence employees’ IUP compliance intention: procedural justice belief and organizational moral climate. Procedural justice belief consists of a set of fairness perceptions employees have regarding the process of organizational decisions (Colquitt 2001). Favorable procedural justice perceptions have been found to facilitate employees’ organizational citizenship behaviors such as helping their work group and improving the quality of their job voluntarily (Tyler et al. 2007). In the same vein, procedural justice would motivate employees to voluntarily comply with the IUP to benefit their organizations.

**H6:** Procedural justice has a positive impact on IUP compliance intention.

Besides the direct impact, procedural justice may indirectly influence IUP compliance intention through influencing the perceived deterrence. Deterrence and organizational justice are not two independent motivating mechanisms for organizational policy adherence. As noted by Tyler (2007), procedural justice will influence employees’ view about the legitimacy of organizational policies and whether the values of their organization are in line with their internal values. Employees may be more willing to devote their time and efforts to better understanding the deterrence mechanisms to avoid the unintended violation of organizational policies. Therefore, we argue that procedural justice could increase the salience of deterrence mechanisms. Employees who perceive justice in security procedures for detecting and punishing Internet abuses are expected to view formal sanctions to be more deterring. Thus, we have

**H7:** Procedural justice has a positive impact on perceived deterrence.

Organizational moral climate is the collective norms of employees regarding personal Internet usage at the workplace. It reflects the moral beliefs shared by most of the employees in an organization. As all individuals depend on others for respect, cooperation and resources, the view of most others or the moral climate will inevitably affect an individual’s construction of meanings of deviant acts including the understanding of deterrence and benefits. For example, moral climate against certain deviant act has been suggested to increase the cost of sanctions, making deterrence more meaningful and salient (Bachman et al. 1992; Wenzel 2004). As a result of the expected reactions from most others in the organization, moral climate against Internet abuses could increase the perceived deterrence of formal sanctions. Similarly, strong disapproval of Internet abuses by most others in an organization may also impede the favorable evaluation of personal Internet usage at the workplace. Thus, we have

**H8:** Organizational moral climate against Internet abuses have a positive impact on perceived deterrence.

**H9:** Organizational moral climate against Internet abuses have a negative impact on perceived benefits.

**Covariates**

In addition to the core constructs mentioned above, we also control for age and gender. In the context of tax compliance, older people were found to be more compliant than younger ones, and women were more compliant than men (Wenzel 2005). Age and gender may also influence employees’ behavior to follow IS security policies such as IUP examined in this study.

**Proposed Research Methodology**

**Preliminary Study Design and Procedure**

The research model is expected to be tested using an online survey delivering to organizational employees in an industrial panel. During the course of writing this article, the authors have already received an approval from the IRB. The first page of the online survey will present an informed consent form, notifying the subjects about the purpose of the study and the completely voluntary and anonymous nature of their participation. Then, all potential participants will be required to answer two filter questions about whether they use the Internet at the workplace and whether they are aware of any IUP in their organization. As our focus is on the compliance of Internet use policy at the workplace, only those who answered “Yes” to both filter questions will be allowed to continue working on the rest of the survey.

---

**Li et al.  Information Systems Security, Assurance, and Privacy Track**

**4**

Twentieth Americas Conference on Information Systems, Savannah, 2014
Variable Measurement

Most of the instruments are drawn from extant studies and re-worded slightly to fit the context of our research, i.e. IUP compliance. Perceived deterrence is measured following the suggestions by Nagin and Paternoster (1993) and Vance and Siponen (2013). Each perceived deterrence measure is computed by multiplying each sanction certainty item by its corresponding sanction severity item. The resulting two perceived deterrence measures reflect both the probability and severity of formal sanctions. Sanction certain and sanction severity are measured using items from Peace et al. (2003). Perceived benefit is measured using items by Li et al. (2010) and Peace et al. (2003). The instrument measuring low self-control consists of eight items from Grasmick et al. (1993) tapping the impulsivity and risk-seeking properties of people with low self-control. Procedural justice is adapted from the studies by Colquitt (2001) and Sindhav et al. (2006). Organizational moral climate is measured using three items adapted after Wenzel (2004). IUP compliance intention is measured using the instruments developed by Limayem et al. (1999) and Peace et al. (2003). All these scales measuring latent constructs, except the perceived benefit, are operationalized as reflective instruments. In line with the study by Li et al. (2010), perceived benefit instrument is implemented as a formative scale. All constructs will be measured on five-point scales.

Proposed Data Analysis Technique, Process, and Expectations

SmartPLS (Ringle et al. 2005), a component-based structural equation modeling (SEM) technique, will be applied as the primary tool to analyze the quality of our measurement model and test the research hypotheses. The use of SmartPLS in our data analysis is largely because of two reasons. First, component-based SEM has minimal demands for residual distributions, which does not assume a multivariate normal distribution and interval scales (Chin et al. 2003). Our research model controlled for gender, which will be coded as a binary variable with 0 and 1 representing female and male, respectively. In addition, PLS is more amenable for handling formative constructs than covariance-based SEM techniques such as LISREL. Perceived benefit will be measured using a formative instrument, which makes SmartPLS particularly suitable for this study. It is expected that we will take a two-stage approach to analyze the survey data. We will first check the measurement quality of those latent constructs and, then perform the path modeling to test our research hypotheses. The SEM analytical results will be presented at the AMCIS conference in this August.

This research progress study is expected to advance IS security research by filling several of the research gaps. First, our study is hoped to confirm the important role of personal traits and organizational context in the rational evaluation of decision process. The cost-benefit assessment varies across individuals and organizational context. The cost-benefit assessment of deviant acts is situational and should not be examined without considering personal traits and organizational context. The integrative approach would help explain some of the inconsistent findings regarding the effect of deterrence in the prior studies (Bulgurcu 2010; Herath and Rao 2009a; Herath and Rao 2009b; Siponen and Vance 2010; Son 2011). Our study shall examine whether or not the organizational context such as procedure justice could influence employees' understanding of deterrence mechanisms. Second, for personal traits, our study will be able to identify and examine the effect of low self-control as both independent force accounting for deviant acts but also as the agent biasing the benefit assessment and its impact on IUP compliance. Third, in terms of organizational context, our study is expected to identify and verify the effect of procedural justice and organizational moral climate on the rational decisional making process. Last but not the least, our integrative research model provides richer insights into the interplay among rational decision process, personal traits and organizational context.

REFERENCES


