Self-control, organizational context, and rational choice in Internet abuses at work

Han Li\textsuperscript{a}, Xin (Robert) Luo\textsuperscript{ab*}, Jie Zhang\textsuperscript{b}, Rathindra Sarathy\textsuperscript{c}

\textsuperscript{a} Robert O. Anderson School of Management, The University of New Mexico, Albuquerque, NM 87131, USA
\textsuperscript{b} Dillard College of Business Administration, Midwestern State University, Wichita Falls, TX 76308, USA
\textsuperscript{c} Spears School of Business, Oklahoma State University, Stillwater, OK 74075, USA

\textbf{ABSTRACT}

Cyber criminals use the Internet as a major platform to launch malware and social engineering attacks. Employees’ violation of Internet use policy (IUP) elevates a firm’s security risks from cyber-attacks. In the literature, such deviant behavior is generally considered to be the result of a cost-benefit calculus. However, this study shows that dispositional factors such as self-control and procedural justice moderate the cost-benefit calculus. We conclude that self-control and procedural justice need to be integrated with the Rational Choice Theory to better explain Internet abuses at work.

\textbf{1. Introduction}

The Internet has revolutionized the way organizations communicate with their employees, customers, and business partners, significantly boosting connectivity and dramatically improving operational efficiency of businesses. Unfortunately, better connectivity through the Internet is also coupled with the potential for a company to fall victim to security violations. Employees may bypass organizational IT settings and abuse Internet access through various non-work-related activities such as playing games, checking personal e-mails, browsing social networks, and watching online pornography. Worse still, employees may unknowingly download a video with embedded malware or post confidential corporate information on social network sites. Without adequate Internet use control and management, personal Internet use at the workplace not only burdens an organization’s IT budget but also exposes it to potential security risks and threats [40].

Internet abuse/misuse, also called cyberloafing, non-work-related computing or workplace Internet deviance, refers to employee intentional use of Internet technology provided by the organization for personal purposes [65]. They may or may not be driven by malicious intent of employees to harm their parent organizations. To deter employee Internet misuse or abuse, Internet use policy (IUP), as one type of information security policies, is leveraged as an essential kind of security management mechanism by the majority of organizations [7]. Advancing the strategic interests of organizational information technologies, an IUP provides employees with guidelines on acceptable and unacceptable Internet use and sanctions for Internet abuses. Despite the wide implementation of the IUP in organizations, a recent study by Palo Alto Networks reveals a significant increase in personal Internet use in organizations [40]. Recent statistics indicate that sixty-four percent of employees visit non-work related websites every day during work hours [23]. Also, US employees averagely spend sixty to eighty percent of their online time on non-work-related activities at the workplace [61]. The astonishing evidence suggests that the deviant Internet usage at the workplace is a top concern of information security management, but also points to the ineffectiveness of IUP as over fifty percent of companies have fired workers for email and Internet abuse [21].

In recent years, deficient compliance with IS security policies has drawn mounting interest in the IS community. Some of these studies have employed such theoretical lens as protection motivation theory and/or general deterrence theory, providing overall support for fear-based mechanisms to ensure compliance such as formal and informal sanctions and the potential for security risks to organizations [14,26,39,54]. Recent studies have attempted to complement the deterrence approach with other theories. For example, Bulgurcu et al. [5] proposed a rational choice framework and empirically verified the competing influence of both cost and benefit factors including sanctions. Siponen and Vance [55], by drawing upon the neutralization theory, empirically verified the effect of neutralization techniques or justifications that employees leverage to defend their violation of security policies. The research models in Siponen and Vance [55] also include formal sanctions as independent drivers for general security policy compliance. However, formal sanctions as fear-based mechanisms were not significant in their study.

\*: Corresponding author.
E-mail address: xinluo@unm.edu (X.R. Luo).
Despite these prior research efforts, the extant literature mostly focuses on IS security policy compliance in general without differing specific types of security violations and policies. As pointed out by Willison and Warkentin [66], different security measures are required for different types of security violations. Siponen and Vance [55] provided empirical evidence that security policy contexts/scenarios matter when studying compliance intention. The focus on general security policy compliance, to certain extent, limits the theoretical richness of current research findings and the practical applicability for effective design and enforcement of specific types of security policies. Considering the escalating scope of IUP violation and limited extant research effort, we focus on the compliance of IUP to unveil its specific driving forces and their interrelationships. Besides the focus on IUP, our study further advances the literature of IS security policy compliance by proposing and testing an integrative model based on multiple theories to explain IUP compliance. Until now, there is a paucity of fine-grained scientific investigations of the relationships between the rational decision-making process and supplementary constructs from additional indispensable theoretical underpinnings in IS security literature. A further integrative understanding of the effect of organizational contexts and personal traits vis-à-vis the occurrence of deviant behavior is still rather scarce in IS security. While the study by Bulgurcu et al. [5] represents such integrative effort in the context of general IS security policy (ISP) compliance, rational choice theory (RCT), personal traits (i.e. self-efficacy), and normative beliefs were combined with the framework of Theory of Planned Behavior as three parallel forces influencing ISP compliance. The findings of their study support the central role of RCT and, more interestingly, unveil the pressing need to complement RCT with other potential factors to explain IS security behaviors. In the literature of criminology, RCT has been proven to be a useful framework for incorporating personal differences and contextual factors to gain a comprehensive understanding of various crimes [37,42]. For example, Paternoster and Simpson [42] suggested that, besides the perceived benefits and sanction threats, intentions to commit corporate crime are subject to the influence of individual propensity to offend and components of organizational context such as the extent of tolerance of a given crime in an organization. Criminal decision making varies with their individual characteristics as well as various situational factors [4].

Following the similar integrative effort by Bulgurcu et al. [5] and studies in the criminology literature, we identified self-control, a personal trait construct from the general crime theory [22], and perceived procedural justice, an organizational context factor from organizational justice literature [13], as two salient factors that may influence employees’ rational decision-making process for IUP compliance. In essence, these two factors have received far less attention than fear-based mechanisms and rational calculus in IS security literature. D’Arcy and Herath [15] have comprehensively examined the most prevalent theoretical underpinnings for behavioral information security research in IS literature and called for additional studies on the e
toretical underpinnings for behavioral information security research in IS literature.

In the following subsections, we first employ the Rational Choice Theory to extract the perceived benefits of performing Internet abuses and the effect of deterrence. Thenceforward, we investigate the role of self-control and procedural justice vis-à-vis IUP compliance via the lens of rational choice.

2.1. Rational choice theory and IUP compliance

IUP violation can be considered a kind of deviant acts. In criminology literature, RCT has been widely applied to explain deviant behaviors in many contexts such as juvenile delinquency, theft, drunk driving, income tax evasion and corporate crimes [42]. One of the core premises of RCT is that potential offenders assess the costs and benefits of alternative courses of actions and try to choose the best alternative [42]. In line with this core premise, employees are likely to violate IUP if the risks such as those from formal sanctions can be outweighed by the perceived benefits of performing deviant acts. Another core premise of RCT highlights the subjective nature of potential offenders’ expectations about reward and cost. The effect of subjective assessment of employees will inevitably be tainted by their stable personal traits such as their inherent ability to control the impulse to engage in deviant acts. For example, Pogarsky [47] found that individuals respond differently to deterrence and emphasized the important role of individual differences played in the deterrence assessment by would-be offenders.
دریافت فوری
متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات