Information & Management 55 (2018) 358–367

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im

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

Han Li[a], Xin (Robert) Luo[a,*], Jie Zhang[b], Rathindra Sarathy[c]

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

ARTICLE INFO

Keywords:
Internet abuses
Rational choice
Self-control
Justice

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.

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).

http://dx.doi.org/10.1016/j.im.2017.09.002
Received 20 September 2016; Received in revised form 27 July 2017; Accepted 3 September 2017
Available online 07 September 2017
0378-7206/

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 effect of self-control on the relationship between sanctions and IS security behaviors. In a similar vein, Hu et al. [28] suggested that it is of paramount importance to further investigate the role of self-control in different settings of information systems security. Whereas Internet access is nearly ubiquitous in today's workplace and presents constant and immediate temptation to employees, no prior studies in IS have investigated the effect of self-control in the context of Internet use policy compliance. Compared with other information security policies, non-compliance with Internet use policy brings employees unique immediate benefits (e.g., excitement and more interesting work life). In this context, self-control is especially relevant. Weak self-control manifested as people's impulsiveness to take immediate benefits may play a particularly salient role in such context. Those with weak self-control may abuse the Internet at the workplace largely under the influence of impetus for immediate benefits while overlooking the potential organizational sanctions. Also, the excitement and thrill from personal Internet activities at work may help satisfy the risk-seeking property of those with weak self-control.

Perceived procedural justice in designing and enforcing IUP is another salient factor that may influence employees' rational thought processes to perform Internet abuses. Workplace injustice has been suggested to generate employee disgruntlement and be used by employees to rationalize their violation of security policies [55,66]. Employees tend to violate information security policies that are unreasonable or illegitimate [55]. The justice perspective is particularly valuable in IUP compliance context considering the astonishing wide scope of Internet abuses at work. Employees seem to cast more doubt on the justice of IUP than other security policies such as confidential data security policy. They may not agree upon what constitutes fair Internet use and the procedures for detecting and punishing violations. The focus on the perceived procedural fairness of IUP is expected to bring forth salient insights into its role in employees' rational thought processes. We are cognizant that no extant studies have investigated the contingent effect of organizational justice on employees' cost-benefit assessment involved in IS security policy compliance.

Therefore, this study proposes and tests an IUP compliance model using RCT as the overarching framework in which the cost-benefit calculus is moderated by employee self-control and perceived procedural justice. The following two questions are addressed in this study. 1) How does procedural justice influence the relationship between cost-benefit assessment and IUP compliance? 2) How does self-control influence the relationship between cost-benefit assessment and IUP compliance? This study goes beyond the parallel integrative perspective taken in prior studies and incorporates the multiplicative effects of self-control and procedural justice. We expect this particular approach to help researchers and practitioners more holistically understand employees' decision-making process to commit IS misuse and uncover new ways to mitigate IUP violations beyond the traditional deterrence approach.

2. Theoretical foundation

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.

In addition, the effect of subjective assessment will also be influenced by the organizational context in which employees form their subjective expectations [42]. The rational choice perspective focuses on *situational* enticements and impediments to offending as well as potential offenders' *subjective cost-benefit assessment* [37]. RCT, as one type of situational theories of crime, emphasizes the importance of context on offender decisions. Prior studies applying RCT have attempted to study a multitude of contextual factors such as the overall economic health of an organization, the existence of organizational resources like reporting hotline and ethical training [42]. Thus, the calculative process underlying the deviant act will vary not only across offenders but also across offense situations (i.e., organizational contexts).

From above, the two core premises of RCT provide it unique advantages over other theories to serve as the overarching framework for incorporating multiple processes driving the deviant act. As such, stable personal trait and organizational contextual factors could be seamlessly integrated with the cost-benefit calculus under the regime *of subjective assessment*.

2.2. Self-control and RCT

In the general crime theory developed by Gottfredson and Hirschi, self-control is considered the enduring propensity to commit deviant acts [22]. One base assumption of the theory is that crimes and analogous behaviors provide easy and immediate gratification. Those lacking self-control would be unable to resist the tempt to commit crimes. The theory posits that "individuals with high self-control will be substantially less likely at all periods of life to engage in criminal acts while those with low self-control are highly likely to commit crime" . The overall inverse relationship between self-control and deviant acts has received fairly consistent support [48].

Despite differences in their central premise, both RCT and general crime theory [22] place importance on the subjective nature of decisions to offend. RCT is essentially a subjective utility theory emphasizing the *subjective* assessment or perceptions of costs and benefits involved in decisions to offend [42]. The salience of perceived cost and benefits could vary by an individual's enduring personal differences. Bouffard argued that "individual factors impact the perceived relevance of several cost and benefit types, even among a relatively homogenous sample of college students" . In line with this view, prior studies have attempted to incorporate a stable propensity (i.e., self-control) into RCT [29,37]. Such integration is important to have a more comprehensive understanding of employee's decisions to violate the IUP. All actors are considered rational and motivated to conduct deviant acts to gratify their self-interests given the access to opportunities. However, individuals have different levels of self-control, which determines, to certain extent, whether one would actually become an offender. Individuals lacking self-control were found to be less influenced by deterrence [38]. They tend to be more enticed by benefits while overlook potential risks, increasing their chance to commit deviant and high-risk acts [22].

2.3. Procedural justice and RCT

In this study, we examine procedural justice in designing and enforcing IUP as one of the organizational contextual factors influencing employees' IUP compliance intention. Procedural justice belief consists of a set of fairness perceptions employees have regarding the process of organizational decisions [13]. Procedural justice has received strong support across various contexts in influencing the decision-making processes for rule compliance [58,59]. Favorable procedural justice perceptions have been found to facilitate employees' organizational citizenship behaviors such as helping their work group and improving

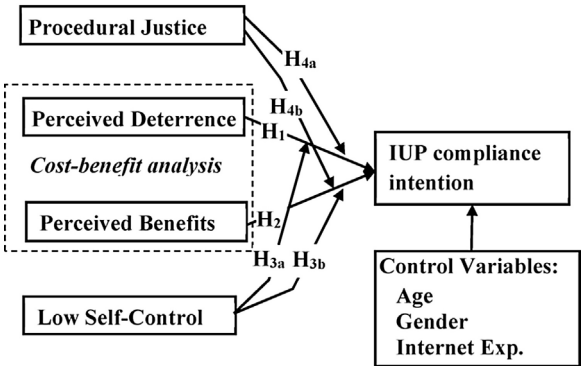

Fig. 1. Research model.

the quality of their job voluntarily [60]. Conversely, unfavorable procedural justice perceptions give rise to undesirable behaviors such as stealing from the employer [11]. Lim [33] found that individuals who feel unfairly treated are more motivated to invoke neutralization techniques to rationalize their subsequent engagement in Internet abuse. In the context of general security policy compliance, Siponen and Vance suggested that employees could rely on neutralization technique to rationalize their violation of security policies that are deemed unfair [55].

Despite the recognition of the effect of justice on the thought process, little if any existing IS security studies have attempted to integrate RCT and procedural justice to examine how justice entangles the cost-benefit analysis or the core of RCT. Thus, the examination of interaction between procedural justice and rational thought process in our study provides a unique perspective for understanding IUP compliance. Organization justice is considered as one of the primary self-regulatory mechanisms for invoking voluntary compliance of policies and regulations [58] while the cost-benefit calculus stands for the instrumental forces. Instrumental forces often, but not always, explain people's compliance behavior [41]. Prior studies have provided some evidence supporting the interaction between self-regulatory approach and instrumental force [52]. The instrumental forces could become less pertinent when individuals become self-regulatory or voluntarily follow rules. Therefore, we argue that the effect of cost-benefit calculus on IUP compliance is contingent upon the perceived justice in designing and enforcing IUP.

3. Research model

Fig. 1 shows the research model of this study. IUP compliance intention is hypothesized to be a consequence of a cost-benefit tradeoff analysis, influenced by the level of self-control in committing (or refraining from) deviant acts, and procedural justice. The following subsections elaborate each of the forces and their associated hypotheses in details.

3.1. Perceived deterrence

In the IS literature, deterrence has been widely examined as an important mechanism to combat computer resource abuses [16,56], reduce software piracy [27], and increase compliance to security policies [26,29,62]. Deterrence consists of two core dimensions: sanction certainty and sanction severity [56]. The former is the perceived probability of being caught for performing deviant acts while the latter refers to the perceived severity of formal sanctions. Both dimensions are important for determining the effectiveness of the deterrence mechanism [62]. Deterrence mechanisms serve 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, we hypothesize that:

H_1. Perceived deterrence increases IUP compliance intention.

3.2. Perceived benefits of Internet abuses

RCT assumes that decisions to perform deviant acts entail an assessment of the deterrence risks and benefits of rule breaking [42]. Sufficient benefits from rule breaking are expected for potential offenders to be willing to undertake the risks of formal sanctions. The benefits include intrinsic as well as extrinsic benefits. For personal Internet use at work, the intrinsic benefits could involve a more interesting work life from personal Internet usage [44]. For example, employees may connect with their friends through Facebook, play online games, or watch entertainment videos at the workplace. Extrinsic benefits could be convenience or savings in terms of cost and time over that of private Internet access [44]. These perceived benefits serve as situational enticements motivating employees to abuse the Internet access at their workplace, reducing their intention to comply with the IUP. Thus, we hypothesize:

H_2. Perceived benefits of Internet abuses decreases IUP compliance intention.

3.3. Self-control

Self-control is a type of predisposition established early in life and remaining stable over one's life [22]. Prior studies have selected different elements to measure self-control for different types of deviant acts. For example, Burton et al. [6] selected impulsivity, risk-seeking, temper, and physicality as the elements of people with weak self-control in adults of a community. Piquero et al. [46] included impulsivity, risk-seeking, volatile temper, and hyperactivity to study convicted criminal offenses such as theft, robbery, etc. Hu et al. [29] incorporated impulsivity, risk-seeking, and self-centeredness to investigate general IS security policy violation by organizational employees. Impulsivity and risk-seeking are common to these studies and seem to be the most important core elements of self-control across different research contexts. This is in line with the comment by Gottfredson and Hirschi that people low in self-control are attracted to deviant acts that are "risky or thrilling" and immediately gratifying . Impulsivity to short-term values and risky decisions associated with people in low self-control has also been found to relate to the prefrontal cortex of human brains using neuroscience methodologies [28]. Therefore, in this study, impulsivity and risk-seeking were selected as the descriptive elements of self-control to examine Internet abuses at the workplace.

Until now, IS security studies have largely examined the additive impact of deterrence and perceived benefits, implicitly assuming that their effects are uniform across individuals [15]. However, prior studies on deterrence in the literature of criminology suggest that the effect of deterrence could vary radically from individual to individual [30,36,49]. Self-control may serve as a contingency variable moderating the effect of deterrence and perceived benefits. Individuals who have weak self-control are fairly unresponsive to sanctions [49] but more responsive to tangible stimuli in the immediate environment and more enticed by short-term gratification [22,25]. In the context of our study, employees with weak self-control would be more enticed by the benefits of personal Internet use at work while paying little attention to potential sanctions. On the other hand, those with strong self-control are less impulsive and risk-seeking, which is in line with the findings of recent neuroscience research in that high self-control individuals tend to activate more neural processes in human brains, spend more time to make a decision, and choose less risky choices [28]. As a result, the potential risks from sanctions may play a more important role in IUP compliance decision for employees with strong self-control while the effect of benefits of Internet abuses may be more salient for employees with weak self-control. Thus, we hypothesize that:

H_{3a}. The relationship between deterrence and IUP compliance intention is moderated by self-control, such that the positive impact is stronger for those with strong self-control.

H_{3b}. The relationship between the perceived benefits of Internet abuses and IUP compliance intention is moderated by self-control, such that the negative impact is stronger for those with weak self-control

3.4. Procedural justice belief

Procedural justice refers to the perceived fairness of processes for making decisions [13]. Various fairness criteria have been suggested for defining procedural justice. Thibaut and Walker [57] proposed two criteria: process control (i.e. the ability to control the process by having a voice) and decision control (i.e. the ability to influence the actual outcome) in a legal setting. Additional criteria were then advocated by Leventhal [31] in more general situations, such as consistency, lack of bias, accuracy of information, correctability, representation, and ethicality. In this study, we select consistency and lack of bias as the fairness criteria for defining procedural justice as we are interested in whether security procedures for detecting and punishing Internet abuses are designed fairly and implemented consistently to everyone in an unbiased manner.

Besides personal traits, the impact of cost-benefit calculus may also be conditional on organizational justice. This line of thinking is supported by the theoretical establishment of organizational justice as one of the key self-regulatory mechanisms for organizational policy compliance [60]. When employees perceive a high level of procedural justice, they would be more likely to regard the organizational policies as legitimate and be more willing to adhere to them *voluntarily* [60]. Such voluntary self-regulation based on procedural justice could downplay or even override the effects of deterrence and the perceived benefits of deviant acts. For example, in the context of tax evasion, deterrence was found to have a stronger effect on those taxpayers who perceived the tax system to be unfair than those perceiving fairness in the tax systems [52]. Extending this theoretical aspect to the context of IUP compliance, it is reasonable to expect that the effects of deterrence and perceived benefits are contingent on procedural justice such that their effects on IUP compliance are more evident in the existence of low procedural justice. Thus,

H_{4a}. The relationship between deterrence and IUP compliance intention is moderated by procedural justice, such that the positive impact is stronger for those who perceive low procedural justice.

H_{4b}. The relationship between perceived benefits and IUP compliance intention is moderated by procedural justice, such that the negative impact is stronger for those who perceive low procedural justice.

3.5. Control variables

Besides the above core constructs, we also controlled for age, gender, and Internet experience in terms of the number of years using Internet. In the context of tax compliance, older people were suggested to be more compliant than younger ones and women were more

Table 1
Demographic Characteristics.

Employee Characteristics						Firm Size (# of Employees)	
Gender		Age		Job Position			
Male	55%	< 20	1%	Executive/ Manager	22%	1–10	3%
Female	45%	20–29	29%	Professional/ Technical	39%	11–250	21%
		30–39	25%	Sales	8%	251–500	15%
		40–49	19%	Clerical	17%	501–1000	12%
		50+	26%	Other	14%	1000+	49%

compliant than men [63]. Age and gender may also influence employees' behavior to follow IS security policies such as the IUP examined in this study. People with more Internet experience tend to have higher self-efficacy in information security and they are likely to demonstrate such capabilities in security compliance behaviors [64]. Therefore, Internet experience may also influence employees' IUP compliance behavior.

4. Methodology

4.1. Research design and procedure

Our research model was tested using an online survey delivered to organizational employees in a panel operated by Zoomerang, a leading survey administration and management company. The company uses a patent-pending technology called "true sample technology" to validate survey responses to ensure that each survey respondent is unique, real, and engaged [51]. The panel service of Zoomerang has been used in several studies published in prestigious IS journals [1,2]. In the end, we received a total of 238 usable responses. To address the possible issue of nonresponse bias, we applied the method suggested by Armstrong and Overton to compare the first and fourth quartile response [9]. In particular, age, gender, and Internet experience were compared using independent sample *t*-test. No significant differences were found between the responses of these two quantiles. Therefore, nonresponse bias should not be an issue for this study.

The demographic characteristics of these survey respondents are shown in Table 1. 55% of them are male and 45% are female, reflecting the typical age distribution of organizational employees. They are mostly between 20 and 49 years old and work as managers, professional/technical people, clerks, and salesperson in firms of different sizes. The respondents represent a nationwide sample of Zoomerang panel and are from many diverse organizations. The distribution of firm sizes indicates a good coverage of firms of different sizes. Overall, these demographic characteristics suggest that our subjects are quite heterogeneous, which, to certain extent, helps increase the external validity of this study.

4.2. Variable measurement

The majority of the instruments were adapted from extant studies with slight rewording to fit the context of our research, i.e. IUP compliance. Instruments measuring sanction certainty and sanction severity were after Peace et al. [43]. Perceived deterrence was measured using the multiplicative approach recommended by Nagin and Paternoster [37] and Vance and Siponen [62]. Each perceived deterrence measure was computed by multiplying each sanction certainty item by its corresponding sanction severity item. The resulting two perceived deterrence measures, i.e. DetPro1*SanSev1 and DetPro2*SanSev2, reflect both the probability and severity of formal sanctions. The multiplicative approach has a sound theoretical basis as rational actors jointly consider the risk and cost of perceived deterrence [15]. A formal sanction is deterring only under the combined presence of both sanction certainty and sanction severity. Perceived benefit was measured using items by Li et al. [32] and Peace et al. [43]. The instrument measuring self-control consists of eight items from Grasmick et al. [25] tapping the impulsivity and risk-seeking properties of people who are low in self-control. Procedural justice was adapted from the studies by Colquitt [13] and Sindhav et al. [53]. Items measuring IUP compliance intention were developed by Limayem et al. [34] and Peace et al. [43]. All these scales, except the perceived benefit, were operationalized as reflective instruments. The perceived benefit instrument was implemented as a formative scale following the criteria suggested by [45]. Perceived benefit scale consists of four items, i.e. save personal time, save personal expense, convenience, and more interesting work life. These items do not covary. For example, an increase in saving personal time is not necessarily accompanied with an increase of other three items. Moreover, each item of perceived benefit scale captures a unique aspect of the content domain of perceived benefits. The four moderation terms formed by self-control and procedural justice were created by applying the product-indicator approach by Chin et al. [10].

All original items were on a five-point scale except the two items of perceived deterrence computed using the multiplicative approach. The values of the two items tapping perceived deterrence vary from 1 to 25. Later in the data analysis stage, the scores of all measurement items including the ones for perceived deterrence were standardized before they were used to test the measurement model and perform path modeling.

5. Data analysis

SmartPLS [50] was applied as the primary tool to analyze the quality of our measurement model and perform hypothesis testing. The use of SmartPLS in our data analysis is largely because of two reasons. First, PLS, as a component-based SEM technique, has minimal demands for residual distributions, and does not require a multivariate normal distribution or interval scales [10]. Our research model controlled for gender, which was coded as a binary variable with 0 and 1 representing female and male, respectively. In addition, PLS is more appropriate for analyzing formative constructs than covariance-based SEM tools such as AMOS and LISREL. Perceived benefit was measured using a formative instrument, which makes SmartPLS particularly suitable for this study. In the following subsections, we took a two-stage approach to analyze the survey data. We first checked the measurement quality of those latent constructs and, then performed the path modeling to test our research hypotheses.

5.1. Measurement model

In this section, we first analyzed the quality of the formative

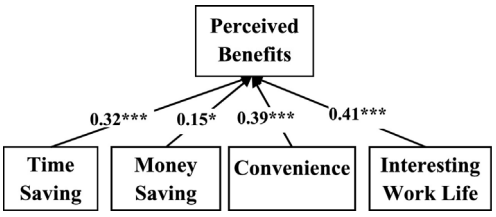

Fig. 2. The relationship between perceived benefit and its measurement items. Completely standardized PLS weights, *p < 0.05, ***p < 0.001.

Table 2
Loadings of measurement instruments.

		Loadings			
Constructs/Items		1	2	3	4
1. Deter	Deter1	**0.94**	0.09	0.31	0.22
	Deter2	**0.94**	0.17	0.35	0.27
2. LSC	LSC2	0.14	**0.75**	0.13	−0.14
	LSC3	0.08	**0.65**	0.17	−0.07
	LSC4	0.15	**0.72**	0.11	−0.09
	LSC5	0.15	**0.77**	0.08	−0.09
	LSC6	0.09	**0.87**	0.06	−0.13
	LSC7	0.10	**0.81**	−0.01	−0.11
	LSC8	0.05	**0.75**	0.07	−0.05
3. ProJus	ProJus1	0.35	0.10	**0.91**	0.36
	ProJus2	0.32	0.10	**0.95**	0.35
	ProJus3	0.30	0.10	**0.88**	0.34
4. Intent	Intent1	0.18	−0.08	0.23	**0.84**
	Intent2	0.29	−0.13	0.38	**0.95**
	Intent3	0.23	−0.13	0.41	**0.92**

Deter − perceived deterrence; LSC − low self-control; ProJus − procedural justice; Intent − intention to comply with Internet use policy.

Table 3
Discriminant Validity of Measurement Model.

	CR	AVE	1	2	3	4
1. Deter	0.94	0.88	**0.94**			
2. LSC	0.91	0.58	0.14	**0.76**		
3. ProJus	0.94	0.84	0.35	0.11	**0.91**	
4. Intent	0.93	0.82	0.26	−0.13	0.38	**0.90**

Note: Elements on the diagonal are the square root of the AVE. Other elements are the correlations among constructs.

instrument for measuring perceived benefit before checking the reliability and validity of those reflective instruments. The quality of the formative instrument was evaluated following the guidelines suggested by MacKenzie et al. [8] and Diamantopoulos and Winklhofer [18]. We first examined the weights of items in perceived benefit. The weights are significant for all four items in perceived benefits (Fig. 2). We further computed variance inflation factor (VIF) statistics for the four items to test the extent of multicollinearity. The computed VIF statistics were found to be between 1.36 and 2.01, which are far below 3.3, the recommended cutoff for formative measures by Diamantopoulos and Siguaw [17]. Therefore, multicollinearity should not be a concern here.

The measurement quality of reflective instruments was then evaluated based on their reliability and validity. An instrument is considered to have convergent validity if all its outer loadings are 0.60 or higher and statistically significant [20]. All item loadings were found to be significant at 0.001 level and above 0.6 except one reversely-worded item in low self-control scale (LSC1). LSC1 was then dropped from subsequent data analysis. The results of PLS modeling after dropping LSC1 were provided in Tables 2 and 3. From Table 2, all reflective instruments have satisfactory convergent validity. To establish reliability, a scale should have its composite reliability (CR) above 0.7 and its average variance extracted (AVE) above 0.5 [3]. From Table 3, all these reflective scales were reliable. To evaluate discriminant validity, we examined the outer loading and cross-loading matrix and the correlation among latent variables. Discriminant validity is supported if the outer loadings of an instrument on their respective construct are higher than its cross loadings on other constructs. The second commonly used discriminant validity criterion requires the square root of each construct's AVE to be higher than the correlations of that construct with any other constructs [19]. As shown in Tables 2 and 3, all reflective instruments satisfy the criteria for discriminant validity.

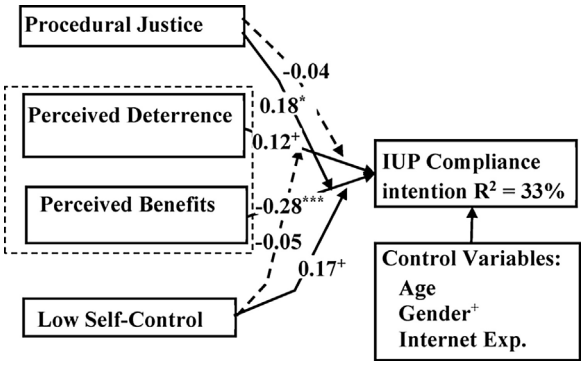

Fig. 3. Hypotheses testing using PLS. Dashed lines indicate insignificant paths with $p > 0.1$. Completely standardized estimates displayed on each path, $^{+}p < 0.1$, $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$ (two-tailed).

In this study, a single survey was used to collect data for all latent constructs at one point in time, which may introduce bias due to common method variance (CMV). The extent of CMV was assessed using the partial correlation procedure [35]. In particular, we evaluated the magnitude of CMV as well as its impact on correlation among constructs. The second smallest positive correlation in the correlation matrix of the manifest variables was selected as a more conservative estimate of CMV (i.e. r_m). r_m was found to be 0.004, which was then used to compute CMV-adjusted correlations among latent constructs by partialing out r_m. CMV-adjusted correlations were only slightly different from the original correlations with differences less than or equal to 0.005. The significance levels for all correlations remain the same. Therefore, CMV should not be a significant issue in our measurement model.

5.2. Hypothesis testing

All main effect paths and the four moderation paths were entered into the model simultaneously with the control variables in the SmartPLS analysis. The results of hypothesis testing were summarized in Fig. 3. Statistical significance was assessed based on t-statistics computed from 500-sample bootstrap procedure with construct level sign changes.

Among the three control variables, gender is marginally significant ($p < 0.1$) with male employees being more compliant with the IUP. The effect of gender found here is opposite to that by Wenzel [63], which may be caused by the differences in research context. The study by Wenzel focuses on the compliance of tax laws. Male and female may respond differently to organizational policies versus governmental laws.

From Fig. 3, the two interaction paths of deterrence (H_{3a} and H_{4a}) are not statistically significant. All other research hypotheses are marginally significant to significant. Therefore, the research model is well supported. Then, we analyzed the two interaction effects that are marginally significant to significant, i.e. H_{3b} and H_{4b}, in details to evaluate the effect size and interaction pattern. The interaction term between self-control and perceived benefits increases the model R^2 value from 0.311 to 0.333 and the one between procedural justice and perceived benefits increases the model R^2 value from 0.301 to 0.333. The effect size of interaction (f2) is 0.032 for the former interaction term and 0.046 for the latter. Both of the effect size values are higher than the 0.02 cutoff for small effect size [12].[1] Hence, we could conclude that self-control and procedural justice do moderate the impact of

[1] $f^2 = [R^2$ (interaction model) $- R^2$ (main effects model)$]/[1 - R^2$ (main effects model)$]$.

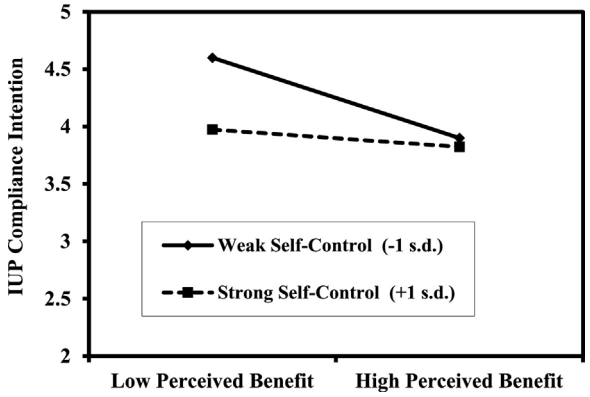

Fig. 4. The interaction pattern between low self-control and perceived benefits.

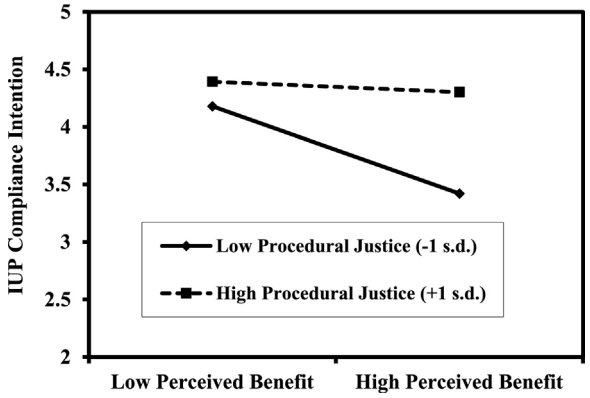

Fig. 5. The interaction pattern between procedural justice and perceived benefits.

perceived benefits on IUP compliance intention.

The interaction effects are shown in Figs. 4 and 5. Perceived benefits significantly reduce IUP compliance intention for employees with weak self-control but not for those with strong self-control. In addition, the negative relationship between perceived benefits and IUP compliance intention is significant in the existence of low procedural justice but not under high procedural justice. Both patterns are consistent with the hypotheses. Therefore, H_{3b} and H_{4b} were supported.

6. Discussion

6.1. Summary of key findings and limitations

Our study examined Internet abuses in the workplace incorporating the effect of personal differences and organizational contexts into RCT. The perceived benefits and deterrence in employees' decision to comply with the IUP were supported by the results of study, confirming the existing literature about the central role of cost-benefit calculus involved in general security policy compliance [5,29]. IUP compliance is more likely when deterrence risks are overridden by the benefits of personal Internet use at the workplace. It is interesting to note that the effect of perceived benefits seems to be more salient than that of perceived deterrence as suggested by its larger standardized path coefficient and t-statistic value.

At the same time, the intention to comply with the IUP was also influenced by employees' predisposition to commit deviant acts, viz. their personal characteristics in the form of self-control. This finding aligns well with the suggestion by Bulgurcu et al. [5] and Hu et al. [29] regarding the role of personal characteristics. At the same time, our study diverges from the additive approach taken by these prior studies, focusing on the contingency effect. Self-control was found to adjust the impact of perceived benefits on IUP compliance intention. Perceived benefits significantly reduce IUP compliance intention only for those employees with weak self-control.

Our results also support the *situational* nature of cost-benefit assessment involved in IUP compliance decisions. The subjective cost-benefit analysis of Internet abuse is influenced by organizational context. In particular, the perceived justice of security procedures was found to moderate the negative impact of perceived benefits on IUP compliance. The negative effect of perceived benefits is stronger in the presence of low procedural justice.

Before discussing the theoretical and practical implications, we point out some of the limitations of this study. First, we only selected two most important core elements including impulsivity and risk-seeking to measure self-control. Future studies may also incorporate the other descriptive elements of self-control to verify the nomological relationships of self-control found in this study. Another limitation is that compliance intention serves as the surrogate for actual compliance behavior in our study. This reflects the typical research practices of recent IS studies on general security policy compliance. However, future studies may be conducted to directly predict actual compliance behavior through collecting employees' self-reported Internet usage in the past or monitoring their actual Internet usage. The former would require researchers to carefully match the survey responses with the actual Internet usage data, which will inevitably expose the identity of survey respondents. Employees would be more reluctant to participate in the study or falsify their answers to some of the survey questions. The self-reported Internet usage behavior at the workplace is also not without caveat. Employees may not truthfully report their actual behaviors considering the sneaky nature of committing deviant acts at the workplace. Lastly, to reflect the behavior of ordinary employees, we studied Internet misuses in general without differentiating malicious use from those without malicious intent. The findings of this study may not be extensible to employees with malicious intent or criminological behaviors. Procedural justice of IUP implementation may play less an important role. Future studies are needed to further test our research model on malicious abuses or e-crime behaviors.

6.2. Theoretical contributions

The primary contribution of our study is the extension of rational choice theory for IUP investigation. The theory was substantially augmented by individuals' personal trait (i.e., self-control) and organizational context factor (i.e., procedural justice) to better explain IUP compliance. In particular, our study identified and confirmed the important roles of self-control and perceived procedural justice in biasing the impact of perceived benefit on the compliance of IUP. The extended RCT is instrumental in elucidating measures organizations could leverage to mitigate the enticing effect of benefits of conducting deviant acts.

This study has several important implications for IS security research. First, our study found that stable individual differences (i.e., self-control) and various situational characteristics including the costs

and benefits of Internet abuses and procedural justice have a joint impact on IUP compliance. Neither situational factors related to offense situations nor individual differences by themselves could sufficiently explain deviant acts. Future IS security studies should put more emphasis on individual differences that may change individuals' subjective evaluation of offense situations. Besides self-control, other personal characteristics may also play important roles. For example, the evaluation of procedural justice and deterrence may be influenced by employees' trust disposition and personal ethical standards.

Second, the findings about self-control provide interesting insights into why rational choice models based purely on cost-benefit analysis fail to explain the non-rational behaviors widely found in prior studies. The behaviors of those with weak self-control seem to be irrational. Our model explains this by showing that self-control could circumscribe the effect of perceived benefits on employees' IUP compliance intention. The effect of perceived benefits of Internet abuses is particularly salient for employees with weak self-control in their IUP compliance decision. However, the effect of self-control may vary with different types of deviant acts across different offender populations. Future studies are needed to validate our model using different samples in the context of other deviant behaviors. For severe crimes, self-control may be far less important than employees' ethical standards and the cognitive assessment of the crime situations.

Finally, the results of our study shed important light on the roles of organizational context on deviant acts. We found high procedural justice inhibits the negative effect of perceived benefits of deviant acts. Our finding highlights the importance of investigating the contingency effect of organizational context in employees' security policy compliance decisions, which has been, by and large, overlooked by current studies in IS literature. Future studies could examine the effect of other organizational contextual factors. For example, information justice emphasizes sharing information on the process and outcome, which may also help increase the salience of deterrence mechanisms.

6.3. Practical implications

This study also has several important practical implications for organizations to reduce Internet abuses. Our study suggests that both deterrence and procedural justice are important levers that motivate employees' IUP compliance. Deterrence mechanisms may need to be supported by fair security procedures and may not be effective otherwise. For example, without the support of procedural justice, deterrence mechanisms may erode the morale of employees and increase their turnover rates. Procedural justice could be enhanced through designing and implementing security procedures in a fair manner. In line with the procedural justice criteria by Thibaut and Walker [57], employers need to allow employees to have a voice and be able to influence the process of designing and implementing security procedures used for detecting and handling Internet abuses. In particular, employers should solicit employee opinions on how much non-work-related Internet usage should be permitted, how Internet usage should be monitored and how severely Internet abuses should be punished. Such an approach would help employees better understand the rationale behind deterrence mechanisms and properly evaluate the sanction risks from Internet abuses. When sanctions against non-work-related Internet usage are enforced, employees should be allowed to defend themselves. Organizations could also follow the principle of consistency to build procedural justice [31]. The security procedures need to be applied consistently to everyone across the entire organization. For example, online activities should be monitored at all levels of organizations including senior managers and those in IT department.

The result of our study also confirms the role of perceived benefits of Internet abuses as an inhibitor of IUP compliance. With respect to perceived benefits, seeking an interesting work life and convenience was found to be the most important benefits of performing non-work-related online activities at the workplace. This is consistent with findings in a recent survey by Salary.com [24] showing that employees waste time at work primarily because they are not motivated enough by their jobs or they feel bored. Employers need to better motivate their employees and, at the same time, create a more interesting work life. These two problems are closely related and need to be addressed hand-in-hand to reduce the time wasted on personal online activities at workplace. Well-motivated employees would enjoy what they do and be devoted to their jobs, thereby perceiving personal online activities to be less beneficial at work.

Another interesting finding of this study is that the effect of perceived benefits is conditioned upon the level of self-control. Weak self-control aggravates the negative impact of perceived benefits on the compliance of IUP. To mitigate the impact of self-control, organizations may need to seek a better match between job and employee personality instead of directly boosting the level of self-control of employees as self-control is one type of stable personal trait established early in life. Specifically, organizations may need to identify those employees with very weak self-control using psychometric instruments such as the one by Grasmick [25] and assign them to jobs that require minimal interaction with the Internet in the workplace such as cashier and maintenance workers. In addition, organizations could use technical approach to mitigate the impact of weak self-control. They could block some of the frequently visited personal sites such as Facebook and Twitter. However, such restrictions may lower employee morale and increase employee turnover rates. Also, the restriction of Internet access on the work computers may not solve the problems as it has become increasingly widespread for employees to use their own mobile devices such as phones or tablets to access non-work-related websites.

IT people are facing growing challenges to expand the security boundary to cover those personal devices. Organizations may lose the battle of controlling personal Internet use at work if they solely rely on technical safeguard measures. Our findings suggest that technical measures need to be supplemented by organizational justice. Employee training needs to be supported by upper management such that managers not only act as the communicators of training messages but also follow the security procedures themselves.

7. Conclusions

With the ever-growing prevalence of social media applications such as Facebook, Twitter, and YouTube, employees are spending excessive time on personal Internet activities at work, which not only raises serious concerns about productivity but also exposes organizations to greater security risks from malware and social engineering attacks. The focus of this study was to understand factors influencing employees' behavioral intention to comply with the Internet Use Policy (IUP). This study presents an integrative model with the Rational Choice Theory as the primary underpinning, augmented by individuals' propensity to commit deviant acts, i.e. self-control and organizational context factors. This research is the first attempt to closely examine employees' comparative evaluation of deviant acts taking into account their personal differences and organizational context. Such an integrative endeavor provides researcher and practitioners with richer insights into the joint effect of multiple forces driving IUP compliance. The results indicate that employees tend to comply with the IUP when the risks of deterrence could be justified by the perceived benefits of personal Internet

use at work. At the same time, such a rational decision process is confounded with the effect of self-control and procedural justice. The impact of perceived benefits on IUP compliance is conditioned upon employees' self-control and procedural justice with their negative effect being more salient for those with weak self-control and in the existence of low procedural justice. The empirical results of this study may also avail IS security management in organizations.

Appendix A

See Table A1

Table A1
Survey Instrument.

Detection Probability [43].	
	If I used the Internet access provided by the organization for non-work- related purposes,
DetPro1	the probability that I would be caught is (Very Low/Very High)
DetPro2	I would probably be caught. (Strongly Agree/Strongly Disagree).
Sanction Severity [43]	
	If I were caught using the Internet access provided by the organization for non-work-related purposes
SanSev1	I think the punishment would be (Very Low/Very High)
SanSev2	I would be severely punished by my organization. (Strongly Agree/ Strongly Disagree)
Perceived Benefit [32,44] (Very Unlikely/Very Likely)	
	Using the Internet access provided by the organization for non-work-related purpose will result in.
PerBen1	Saving my personal time using private Internet access.
PerBen2	Saving my personal expense using private Internet access.
PerBen3	Convenience.
PerBen4	More interesting work life.
Low Self-Control [25] (Strongly Agree/Strongly Disagree)	
LSC1	I devote time and effort to preparing for the future.* (Dropped from the data analysis)
LSC2	I act on the spur of the moment without stopping to think.
LSC3	I do things that bring me pleasure here and now, even at the cost of some future goal.
LSC4	I based my decisions on what will benefit me in the short run, rather than in the long run.
LSC5	I test myself by doing things that are a little risky.
LSC6	I take risks just for the fun of it.
LSC7	I find it exciting to do things for which I might get in trouble.
LSC8	Excitement and adventure are more important to me.
Procedural Justice [13,53] (Strongly Agree/Strongly Disagree)	
ProJus1	The security procedures for detecting and punishing non-work-related Internet usage are applied consistently to everyone in my organization.
ProJus2	The security procedures for detecting and punishing non-work-related Internet usage are applied in a fair manner to everyone in my organization.
ProJus3	The security procedures for detecting and punishing non-work-related Internet usage are designed fairly in my organization.
Intention to Comply with Internet Use Policy [34,43] (Strongly Agree/Strongly Disagree)	
Intent1	I may follow the Internet use policy of my organization in the future.
Intent2	I intend to follow the Internet use policy of my organization in the future.
Intent3	I expect to follow the Internet use policy of my organization in the future.

References

[1] C.M. Angst, R. Agarwal, Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion, MIS Q. 33 (2) (2009) 339–370.
[2] R. Ayyagari, V. Grover, R. Purvis, Technostress: technological antecedents and implications, MIS Q. 35 (4) (2011) 831–858.
[3] R.P. Bagozzi, Y. Yi, On the evaluation of structural equation models, J. Acad. Mark. Sci. 16 (1) (1988) 74–94.
[4] J.A. Bouffard, Predicting differences in the perceived relevance of crime's costs and benefits in a test of rational choice theory, Int. J. Offender Ther. Comp. Criminol. 51 (4) (2007) 461–485.
[5] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rational-based beliefs and information security awareness, MIS Q. 34 (3) (2010) 523–548.
[6] V.S. Burton, D.T. Evans, F.T. Cullen, K.M. Olivares, G.R. Dunaway, Age, self-control, and adults' offending behaviors: a research note assessing a general theory of crime, J. Crim. Justice 27 (1) (1999) 45–54.
[7] CareerBuilder, Half of workers plan to do some online holiday shopping at work, (2012). Last accessed on 2015 October 14 http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=11%2F26%2F2012&id=pr726&ed=12%2F31%2F2012.
[8] CEB, Managing the hidden causes of data breaches, CEB (2016).
[9] CERT, Common Sense Guide to Mitigating Insider Threats, Carnegie Mellon University Software Engineering Institute, 2016.
[10] W.W. Chin, B.L. Marcolin, P.R. Newsted, A partial least squares latent variable modeling approach for measuring interaction effects: results from a Monte Carlo simulation study and an electronic mail adoption study, Inf. Syst. Res. 14 (2) (2003) 189–217.
[11] Y. Cohen-Charash, P.E. Spector, The role of justice in organizations: a meta-analysis, Organ. Behav. Hum. Decis. Process. 86 (2) (2001) 278–321.

[12] J. Cohen, Statistical Power Analysis for the Behavior Sciences, Lawrence Erlbaum, Hillsdale, NJ, 1988.
[13] J.A. Colquitt, On the dimensionality of organizational justice: a construct validation of a measure, J. Appl. Psychol. 86 (3) (2001) 386–400.
[14] R.E. Crossler, J.H. Long, T.M. Loraas, B.S. Trinkle, Understanding the compliance with bring your own device policies utilizing protection motivation theory: bridging the intention-behavior gap, J. Inform. Syst. 28 (1) (2014) 209–226.
[15] J. D'Arcy, T. Herath, A review and analysis of deterrence theory in the IS security: making sense of the disparate findings literature, Eur. J. Inf. Syst. 20 (6) (2011) 643–658.
[16] J. D'Arcy, A. Hovav, D. Galletta, User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach, Inf. Syst. Res. 20 (1) (2009) 79–98.
[17] A. Diamantopoulos, J.A. Siguaw, Formative versus reflective indicators in organizational measure development: a comparison and empirical illustration, Br. J. Manage. 17 (4) (2006) 263–282.
[18] A. Diamantopoulos, H.M. Winklhofer, Index construction with formative indicators: an alternative to scale development, J. Mark. Res. 38 (2) (2001) 269–277.
[19] C. Fornell, D. Larcker, Evaluating structural equation models with unobservable variables and measurement error, J. Mark. Res. 18 (1) (1981) 39–50.
[20] D. Gefen, D. Straub, A practical guide to factorial validity using PLS-graph: tutorial and annotated example, Commun. AIS 16 (5) (2005) 91–109.
[21] N. Gohring, Over 50% of companies have fired workers for e-mail, Net abuse, Comput. World (2008).
[22] M.R. Gottfredson, T. Hirschi, A General Theory of Crime, Stanford University Press, Stanford, CA, 1990.
[23] A. Gouveia, Wasting time at work, (2012). Last accessed on 2015 October 14 http://www.salary.com/wasting-time-at-work-2012/.
[24] A. Gouveia, Wasting Time at Work Survey, (2013). Last accessed on 2014 February, 6 http://www.salary.com/2013-wasting-time-at-work-survey.
[25] H.G. Grasmick, C.R. Tittle, J. RobertJ. Bursik, B. Arneklev, Testing the core empirical implications of Gottfredson and Hirschi's general thoery of crime, J. Res. Crime Delinquency 30 (1) (1993) 5–29.
[26] T. Herath, H.R. Rao, Protection motivation and deterrence: a framework for security policy compliance in organizations, Eur. J. Inf. Syst. 18 (2) (2009) 106–125.
[27] G.E. Higgins, B.D. Fell, A.L. Wilson, Digital piracy: assessing the contributions of an integrated self-control theory and social learning theory usig structural equation modeling, Crim. Justice Stud. 19 (1) (2006) 3–22.
[28] Q. Hu, R. West, L. Smarandescu, The role of self-control in information security violations: insights from a cognitive neuroscience perspective, J. Manage. Inf. Syst. 31 (4) (2015) 6–48.
[29] Q. Hu, Z. Xu, T. Dinev, H. Ling, Does deterrence work in reducing information security policy abuse by employees? Commun. ACM 54 (6) (2011) 54–60.
[30] B.A. Jacobs, Deterrence and deterrability, Criminology 48 (2) (2010) 417–441.
[31] G.S. Leventhal, What should be done with equity theory, in: K. Gergen, M. Greenberg, R. Willis (Eds.), Social Exchange: Advances in Theory and Research, Plenum, New York, 1980.
[32] H. Li, J. Zhang, R. Sarathy, Understand the compliance with the Internet Use Policy from the perspective of rational choice theory, Decis. Support Syst. 48 (4) (2010) 635–645.
[33] V.K.G. Lim, The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice, J. Organ. Behav. 23 (5) (2002) 675–694.
[34] M. Limayem, M. Khalifa, W.W. Chin, Factors motivating software piracy: a longitudinal study, Proceedings of the International Conference on Information Systems, North Carolina United States, 1999.
[35] M.K. Lindell, D.J. Whitney, Accounting for common method variance in cross-sectional research designs, J. Appl. Psychol. 86 (1) (2001) 114–121.
[36] R.E. Mann, R.G. Smart, G. Stoduto, E.M. Adlaf, E. Vingilis, D. Beirness, R. Lamble, M. Asbridge, The effects of drinking-driving laws: a test of the differential deterrence hypothesis, Addiction 98 (11) (2003) 1531–1536.
[37] D.S. Nagin, R. Paternoster, Enduring individual differences and rational choice theories of crime, Law Soc. Rev. 27 (3) (1993) 467–496.
[38] D.S. Nagin, R. Paternoster, Personal capital and social control: the deterrence implications of a theory of individual differences in criminal offending, Criminology 32 (4) (1994) 581–606.
[39] S. Pahnila, M. Siponen, A. Mahmood, Employees' behavior toward IS security policy compliance, 40th Hawaii International Conference on System Sciences, Hawaii, 2007.
[40] Palo Alto Networks, The application usage and risk report − An analysis of end user application trends in the enterprise, (2012). Last accessed on June 25 2015 http://media.paloaltonetworks.com/documents/Application-Usage-and-Risk-Report-9th-Edition.pdf.
[41] R. Paternoster, The deterrent effect of the perceived certainty and severity of punishment: a review of the evidence and issues, Justice Q. 4 (2) (1987) 173–217.
[42] R. Paternoster, S. Simpson, Sanction threats and appeals to morality: testing a rational choice model of corporate crime, Law Soc. Rev. 30 (3) (1996) 549–583.
[43] A.G. Peace, D. Galletta, J. Thong, Software piracy in the workplace: a model and empirical test, J. Manage. Inf. Syst. 20 (1) (2003) 153–177.
[44] L.G. Pee, I.M.Y. Woon, A. Kankanhalli, Explaining non-work-related computing in the workplace: a comparison of alternative models, Inf. Manage. 45 (2) (2008) 120–130.
[45] S. Petter, D. Straub, A. Rai, Specifying formative constructs in information systems research, MIS Q. 31 (4) (2007) 623–656.
[46] A.R. Piquero, T.E. Moffitt, B.E. Wright, Self-control and criminal career dimensions, J. Contemp. Crim. Justice 23 (1) (2007) 72–89.
[47] G. Pogarsky, Identifying deterrable offenders: implications for research on deterrence, Justice Q. 19 (3) (2002) 431–452.
[48] T.C. Pratt, F.T. Cullen, The empirical status of Gottfredson and Hirschi's general theory of crime: a meta-analysis, Criminology 38 (3) (2000) 931–964.
[49] T.C. Pratt, F.T. Cullen, K.R. Blevins, L.E. Daigle, T.D. Madensen, The empirical status of deterrence theory: a meta-analysis, in: F.T. Cullen, J.P. Wright, K.R. Blevins (Eds.), Taking Stock: The Status of Criminological Theory New Brunswick, Transaction Publishers, NJ, 2006.
[50] C.M. Ringle, S. Wende, A. Will, SmartPLS. vol. 2.0 (beta) 2005.
[51] K.E. Rudestam, R.R. Newton, Surviving Your Dissertation: A Comprehensive Guide to Content and Process, SAGE Publications, Los Angeles, CA, 2015.
[52] W.J. Scott, H.G. Grasmick, Deterrence and income tax cheating: testing interaction hypotheses in utilitarian theories, J. Appl. Behav. Sci. 17 (3) (1981) 395–408.
[53] B. Sindhav, J. Holland, A.R. Rodie, P.T. Adidam, L.G. Pol, The impact of perceived fairness on satisfaction: are airport security measures fair? Does it matter? J. Mark. Theory Pract. 14 (4) (2006) 323–335.
[54] M. Siponen, S. Pahnila, A. Mahmood, Factors influencing protection motivation and IS security policy compliance, Innovations in Information Technology, IEEE, Dubai, 2006.
[55] M. Siponen, A. Vance, Neutralization New insights into the problem of employee information systems security policy violations, MIS Q. 34 (3) (2010) 487–502.
[56] D.W. Straub, Effective IS security: an empirical study, Inf. Syst. Res. 1 (3) (1990) 255–276.
[57] J. Thibaut, L. Walker, Procedural Justice A Psychological Analysis, Lawrence Erlbaum, Hillsdale, NJ, 1975.
[58] T.R. Tyler, Restorative justice and procedural justice: dealing with rule breaking, J. Soc. Issues 62 (2) (2006) 307–326.
[59] T.R. Tyler, S.L. Blader, Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings, Acad. Manage. J. 48 (6) (2005) 1143–1158.
[60] T.R. Tyler, P.E. Callahan, J. Frost, Armed, and dangerous (?): Motivating rule adherence among agents of social control, Law Soc. Rev. 41 (2) (2007) 457–492.
[61] J.C. Ugrin, J.M. Pearson, The effects of sanctions and stigmas on cyberloafing, Comput. Human Behav. 29 (3) (2013) 812–820.
[62] A. Vance, M.T. Siponen, IS security violations: a rational choice perspective, J. Organ. End User Comput. 24 (1) (2012) 21–41.
[63] M. Wenzel, Motivation or rationalization? Causal relations between ethics, norms and tax compliance, J. Econ. Psychol. 26 (4) (2005) 491–508.
[64] M.E. Whitman, H.J. Mattord, Principles of Information Security, Thomason Course Technology, Bonston, MA, 2005.
[65] P.-O.H. Wikström, Violence as situattional action, Int. J. Conflict Violence 3 (1) (2009) 75–96.
[66] R. Willison, M. Warkentin, Beyond deterrence: an expanded view of employee computer abuse, MIS Q. 37 (1) (2013) 1–20.

Han Li is an assistant professor of MIS in Anderson School of Management at the University of New Mexico. She received her doctorate in management information systems from Oklahoma State University. She has published in *Decision Sciences*, *Decision Support Systems, Operations Research, European Journal of Information Systems, Information Systems Journal, Journal of Database Management, Journal of Computer Information Systems, Information Management & Computer Security*, and *Journal of Information Privacy and Security*. Her current research interests include health IT, privacy and confidentiality, data and information security and the adoption of information technology.

Xin (Robert) Luo is an endowed regent's professor and associate professor of MIS and information assurance in the Anderson School of Management at the University of New Mexico, USA. He is the associate director of Center for Information Assurance Research and Education at UNM. He received his PhD in MIS from Mississippi State University, USA. He has published research papers in leading journals including *Communications of the ACM, Decision Sciences, Decision Support Systems, European Journal of Information Systems, Information & Management*, *Journal of the AIS, Journal of Strategic Information Systems,* and *Computers & Security*. He is currently serving as an ad hoc associate editor for *MIS Quarterly* and an associate editor for *European Journal of Information Systems, Electronic Commerce Research, Journal of Electronic Commerce Research*, and *International Conference on Information Systems*. His research interests center around information assurance, innovative technologies for strategic decision-making, and global IT management. He is the Editor-in-chief for *International Journal of Information and Computer Security* and coeditor-in-chief for *International Journal of Accounting and Information Management*.

Jie Zhang is an associate professor of MIS in the Dillard College of Business Administration at Midwestern State University. She received her PhD in management information systems from the University of Mississippi. She has published in *Decision Sciences, Decision Support Systems, European Journal of Information Systems, Information Systems Journal, Journal of Computer Information Systems, Information Management & Computer Security*, and *Journal of Information Privacy and Security*. Her research interests include behavioral information security, privacy, and SMEs information systems management.

Rathindra Sarathy is the Ardmore Chair and Professor of Information Systems in the Spears School of Business at Oklahoma State University. He received his Ph.D. from Texas A & M University. He has published in many journals including *ACM Transactions on Database Systems, Decision Sciences, Decision Support Systems, Information Systems Research, Management Science, Information Systems Journal*, and *Operations Research*. His current research interests include privacy and confidentiality, data masking, data and information security, and e-commerce.