doi: 10.1111/isj.12037

Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance

Han Li,* Rathindra Sarathy,† Jie Zhang‡ & Xin Luo§

*School of Business, Minnesota State University Moorhead, Moorhead, MN 56563, USA, email: jie. li@mnstate.edu, †Spears School of Business, Oklahoma State University, Stillwater, OK 74078, USA, email: rathin.sarathy@okstate.edu, ‡Dillard College of Business Administration, Midwestern State University, Wichita Falls, Texas 76308, USA, email: jie.zhang@mwsu.edu, and §Anderson School of Management, University of New Mexico, Albuquerque, NM 87131, USA, email: Luo@mgt.unm.edu

Abstract. *Internet security risks, the leading security threats confronting today's organizations, often result from employees' non-compliance with the internet use policy (IUP). Extant studies on compliance with security policies have largely ignored the impact of intrinsic motivation on employees' compliance intention. This paper proposes a theoretical model that integrates an intrinsic self-regulatory approach with an extrinsic sanction-based command-and-control approach to examine employees' IUP compliance intention. The self-regulatory approach centers on the effect of organizational justice and personal ethical objections against internet abuses. The results of this study suggest that the self-regulatory approach is more effective than the sanction-based command-and-control approach. Based on the self-regulatory approach, organizational justice not only influences IUP compliance intention directly but also indirectly through fostering ethical objections against internet abuses. This research provides empirical evidence of two additional effective levers for enhancing security policy compliance: organizational justice and personal ethics.*

Keywords: internet abuses, information security and privacy, deterrence, organizational justice, ethics

INTRODUCTION

The internet is becoming the *de facto* platform for the cost–effective transmission of business data within a company and among its business constituents. While the internet is universally acknowledged as revolutionizing the way business is conducted in terms of communication efficiency and effectiveness, it may also be deemed a double-edge sword. The internet may be misused by employees at the workplace for non-work related internet activities such as checking personal emails, gaming, shopping, and browsing non-work-related websites. A

recent Gallup poll shows that the average employee spends over 75 min per day on personal internet activities at the workplace. 'The International Data Corp. estimated that 30% to 40% of employee internet use isn't work related' (Schweitzer, 2004). Non-work-related internet use not only results in productivity loss but also exposes companies to increased security breaches such as malware attacks and leakages of corporate and customer confidential information. The Web has become 'the major vehicle for cybercriminals looking to infect computers around the world' (Sophos, 2009). There is a new infected webpage every 3.6 s or 23 500 Web pages every day. These infected Web pages often appear legitimate and are exploited by hackers to spread malware. According to the Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) Security Report, dealing with security issues within the organizational network costs each organization an average of nearly $350 000 in 2008. In addition to the monetary issues at stake, other security incident driven factors such as damaged reputation and privacy backlash from consumers can worsen the devastating aftermath of the impact of security breaches on organizations. This problematic phenomenon has attracted attention in both academic and pragmatic communities.

Most companies have implemented an internet use policy (IUP) as an important part of their security initiative to combat various forms of internet misuses at the workplace (Young & Case, 2004; Webroot, 2010; CareerBuilder, 2012). For example, Webroot (2010) found that 81% of small and medium-sized companies have an IUP with half of them driven by their employees' inappropriate use of social networking sites. However, despite the wide implementation of IUP, the extent of internet misuses is escalating as suggested by the results of a recent survey that average employees in US spend 60–80% of their online time on personal tasks at the workplace (Ugrin & Pearson, 2013). This puts the effectiveness of IUPs in doubt. Enforcing IUPs effectively is imperative for employers to reduce not only productivity loss but also security breaches. Drawing on pertinent organizational justice and deterrence literature, this paper empirically explores how to motivate compliance with the IUP. Prior studies have primarily assumed employees as rational actors wishing to maximize their individual outcomes and have applied this perspective to understand compliance with IS security policies. In particular, they have investigated various mechanisms such as formal and informal controls or sanctions (Boss *et al*., 2009; Bulgurcu, 2010; Li *et al*., 2010; Hu *et al*., 2011; Vance & Siponen, 2012) and neutralization techniques that employees invoke to rationalize their deviant acts (Siponen & Vance, 2010). However, the rationalization-based perspective did not shed light on employees' intrinsic motivations, such as ethical values, underlying the voluntary compliance of organizational rules and policies. As such, we propose a comprehensive framework in a bid to gauge and compare two distinct approaches for achieving compliance: an extrinsic sanction-based approach and an intrinsic self-regulatory approach that considers organizational justice and personal ethics, with an emphasis on the latter approach.

The research model was validated through a survey using 241 organizational employees who are regulated by their companies' IUP. Structural equation modelling was employed to test the proposed hypotheses. In essence, this study carries significant contributions to the literature related to individual's compliance with security policies in an organizational context. Whereas previous research focuses on sanction-based compliance enforcement method, the analytical results of our study suggest that a self-regulatory approach has a much stronger influence over

compliance with the IUP than sanction-based mechanisms. In particular, organizations could use two additional self-regulatory levers to enhance security policy compliance: organizational justice beliefs and personal ethics. Beliefs related to organizational justice were found to have both a direct and an indirect effect through personal ethics on employees' IUP compliance intention.

The remainder of the article unfolds as follows: in the following section, we review the literature to identify gaps in the literature and highlight the unique contributions of our study. In the third section, we lay out the theoretical foundation of our work through applying deterrence theory and organizational justice theory. Following that, we develop our research model and hypotheses. Next, we describe our research methodology and test our research model. We conclude the paper with a discussion of the findings, limitations, contributions, implications to theory and practice, and future research directions avenues.

PRIOR RESEARCH ON IS SECURITY POLICY COMPLIANCE

The prevalence of personal internet usage in the workplace has piqued increasing interest in the Information Systems (IS) research community. The literature has examined the impact of non-work-related computing on job performance (Bock & Ho, 2009) and factors predicting internet abuses (Lim, 2002; Pee *et al*., 2008) such as affect, perceived consequence, habit and organizational injustice. To combat internet abuses, most companies include an IUP as part of their IS security program. In this section, we review below that, although current studies on compliance with IS security policies have made important contributions, the roles of intrinsic motivations or self-regulatory approaches have received little attention.

Studies on IS security policy have applied different theories to explain compliance behaviors. For example, formal sanctions were suggested to improve employee compliance based on general deterrence theory (Pahnila *et al*., 2007; Herath & Rao, 2009a; 2009b). Relying on the control literature, Boss *et al*. (2009) found that perceived mandatoriness of security policies could motivate employees to take security measures. Besides formal sanctions, prior studies have applied protection motivation theory to examine the effects of perceived IS security threat and the efficacy of coping on security policy compliance (Pahnila *et al*., 2007; Herath & Rao, 2009b; Johnston & Warkentin, 2010). These studies have identified several fear-based motivating forces for security policy compliance, including fear of formal sanctions, informal sanctions from relevant others and threats to the organization's security. As extrinsic motivators, fear-based motivational forces increase the compliance intention by increasing the cost of non-compliance. Recent studies have also applied rational choice theory to investigate not only costs but also benefits factored into employees' decision to rationalize their compliance behaviors (Bulgurcu, 2010; Li *et al*., 2010; Vance & Siponen, 2012). With a focus on *non-compliance* of IS security policies, Siponen & Vance (2010) further applied neutralization theory to identify neutralization techniques employees use to rationalize their violation of security policies. These studies link people's behavior to personal gain/loss calculations or excuses justifying their deviant acts rather than to personal values.

By leveraging values, self-regulation has been advocated as an effective mechanism facilitating rule adherence in organizations (Tyler *et al*., 2007). Employee self-regulation is driven by an innate feeling or desire for compliance, i.e. it is an intrinsic motivator (Tyler *et al*., 2007). For example, employees may feel obligated to follow organizational policies as a result of their personal ethics or act in the best interest of their organization to which they are strongly committed. Evidence exists that intrinsic motivators could be more effective than extrinsic motivators in IS security policy compliance (Son, 2011). However, intrinsic motivation has only received sparse research attention in extant IS security studies. Son (2011) found that perceived legitimacy and perceived value congruence, two specific workplace judgments, are strong predictors of IS security policy compliance. In the study of formation and alleviation of employee disgruntlement, Willison & Warkentin (2013) emphasized the role of organizational justice and called for investigating organization justice as the motivator for other end-users security behaviors.

Prior studies have provided valuable insights into the impact of some of the intrinsic motivators on security policy compliance. However, it is not clear whether organizations can leverage self-regulation to facilitate IUP compliance. For example, D'Arcy *et al*. (2009) found that personal moral beliefs play an important role in information systems misuse but did not examine what mechanisms could be used by organizations to engender favorable personal moral beliefs to reduce IS resources misuse. In this study, we aim to integrate extrinsic command-and-control and intrinsic self-regulatory approaches. Moreover, by incorporating organizational justice, we strive to provide an in-depth and comprehensive understanding of the self-regulatory approach.

THEORETICAL FOUNDATION AND HYPOTHESES

In this section, we first build the theoretical foundation of our research model. In particular, we discuss the roles of extrinsic command-and-control approach and two self-regulatory approaches, i.e. personal ethics and organizational justice beliefs. Then, we propose the research model and hypothesize the relationships among constructs.

IUP compliance and command-and-control approach

The command-and-control approach emphasizes the role of extrinsic motivational forces such as sanctions (Tyler *et al*., 2007). It assumes that employees are rational decision-makers and attempt to maximize their outcomes. Rule adherence is argued to be a result of a cost–benefit analysis. Formal sanctions are a type of command-and-control approach widely deployed by organizations to deter deviant behaviours. The risks from formal sanctions influence employees' decisions relating to organizational deviant behaviours (Paternoster, 1987), by increasing the cost of such behaviours. In this study, we empirically examine the influence of the formal sanctions on compliance with the IUP.

IUP compliance and self-regulatory approach

The self-regulatory approach focuses on intrinsic motivations, which operates through the activation of employees' values and feelings of responsibility towards their organizations

(Tyler *et al*., 2007). Rule adherence is considered to arise from an individual's intrinsic desires or feelings of personal obligation to an organization. Prior studies have identified several intrinsic motivational forces for rule adherence, such as value judgments about legitimacy of the organization and its policies and one's moral values (Tyler, 2006; Tyler *et al*., 2007). Workplace judgments such as legitimacy and value congruence have been found important in constituting personal motivation (Son, 2011). In the context of adherence to organizational policies, legitimacy refers to the judgment about whether the organization has the authority or legitimacy to enforce policies. High assessment of organizational legitimacy increases feelings of obligation to comply with organizational policies (Tyler, 2006; Tyler *et al*., 2007). Compliance could also be motivated through the congruence between organizational policies and employee's moral values (Paternoster & Simpson, 1996). Through interviews with organizational managers, moral values were identified as one fundamental means to achieve IS security (Dhillon & Torkzadeh, 2006). In the context of IUP compliance, personal ethical objections against internet abuses are a type of value judgments reflecting whether restricting personal internet use using the IUP is in line with one's ethical views. In this study, we are interested in how employees' moral values on the personal use of the internet at the workplace (i.e. personal ethics against internet abuses) are formed from the perspective of organizational justice and how personal ethics together with organizational justice beliefs motivate the compliance with the IUP.

Organizational justice beliefs are a set of fairness perceptions reflecting employees' assessment about the degree of fairness in the process and outcomes of organizational decisions (Colquitt, 2001). These fairness perceptions have been found to motivate favorable attitudes and behaviors in various managerial settings (Cohen-Charash & Spector, 2001). For example, favorable fairness perceptions about organizational procedures were found to increase employees' willingness to *voluntarily* help their work group and improve the quality of their job performance (Tyler *et al*., 2007). Justice beliefs have been considered a source of intrinsic motivation distinct from one's self-interests to maximize his or her own outcomes, and its impact could even dominate that based on self-interests (Leventhal *et al*., 1980; Lerner, 2003; Tyler *et al*., 2007). Therefore, we argue that justice beliefs serve as another important intrinsic self-regulatory lever, which could directly influence the compliance with the IUP.

Besides the direct impact, organizational justice may also influence IUP compliance indirectly through shaping employees' personal ethics or moral values on the personal use of the internet. This argument is in line with the research findings of Tyler *et al*. (2007) that the influence of procedural justice on rule adherence is primarily explained by its impact on ethical values. Personal ethics, reflecting one's normative expectations about the appropriateness of a situation or action, could be changed through socialization at home or workplace. Employees develop experiences about the processes and rules of their organizations through daily work or training. Such experiences could then shape their attitudes, values and behaviors. Part of the values shared within an organization could be internalized as personal values (Wenzel, 2004), influencing an individual's normative expectations about whether certain deviant act is right or wrong. Organizational justice is one important factor facilitating such internalization of organizational values as personal ethical values as people is concerned about the fair treatment by their organizations, which is indicative of their inclusion and standing in the

group (Wenzel, 2002). The internalization process is more likely to be activated when employees perceive justice in their organizations. Organizational justice would make employees more willing to accept the values of their organization and form a favourable value judgement about organizational policies and comply with them voluntarily (Tyler *et al*., 2007). Therefore, in the context of IUP compliance, we argue that justice beliefs about IUP and its enforcement in an organization would influence employees' personal ethics against internet abuses at the workplace.

To summarize, we can conclude that security policy compliance is driven by both extrinsic and intrinsic motivational forces, i.e. formal sanctions and self-regulation. Formal sanctions and self-regulation have both received support as influencers of policy adherence in prior studies. But, these two approaches are not equally attractive to organizations. In order for formal sanctions to be effective, organizations need to invest considerably in surveillance technology. Also, excessive formal sanctions could hurt the morale of employees and crowd out their intrinsic motivation to comply with organizational policies (Tyler, 2006). Thus, promoting the self-regulation may be especially appealing to authorities.

Based on the previous discussion of research foundation, we propose a research model that explains IUP compliance as the joint effect of formal sanctions and justice-based self-regulatory approaches (Figure 1). The research model suggests that employees' IUP compliance intention will increase when (1) employees perceive high threats from formal sanctions; (2) employees have ethical views against internet abuses; and (3) employees perceive higher level of fairness in IUP policy design and enforcement. The model also suggests that organizational justice could enhance compliance with the IUP indirectly through shaping personal ethical views against internet abuses. The following sections illustrate each of the motivational forces and their impact on IUP compliance intention in more details.

Formal sanctions

Formal sanctions or punishments have been widely studied using deterrence theory to combat individual deviant behaviours in various settings such as tax compliance, street crime and

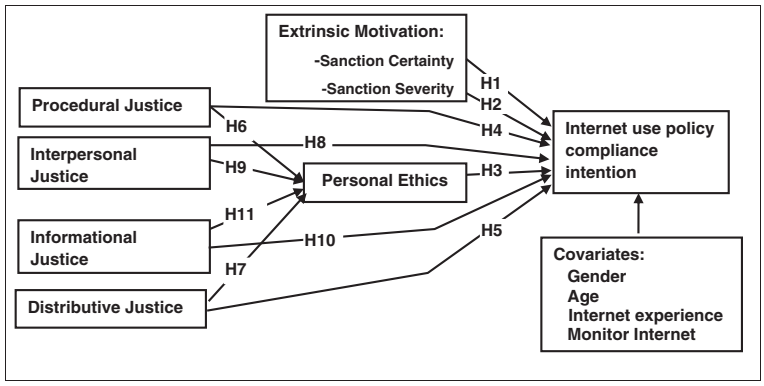

Figure 1. Research model.

corporate offense (Paternoster & Simpson, 1996; Wenzel, 2004). The overall argument from this stream of research is that formal sanctions increase the cost of the deviant act and, therefore, reduce the possibility of deviant acts. Recently, formal sanctions have received growing attention in IS literature for reducing the misuse of IS assets or violation of security policies (D'Arcy *et al*., 2009; Vance & Siponen, 2012). Deterrence has been supported as a useful strategy for reducing computer abuses and software piracy in organizations (Straub, 1990; Peace *et al*., 2003; D'Arcy *et al*., 2009). The deterrence effect of formal sanctions consists of two dimensions: perceived certainty of sanction (or detection probability) and perceived level of sanction severity.

Potential offenders are less likely to follow rules and policies if violations cannot be detected by the organization. A low level of sanction certainty has been identified as an important reason for increased frequency of employee theft (Lau *et al*., 2003) and software piracy (Peace *et al*., 2003). In this study, perceived sanction certainty is employees' perception of the probability that they will be caught if they use the internet access provided by the organization for personal purposes. The prevalence of personal internet usage at the workplace implies a large population of potential offenders of IUP. High sanction certainty clearly increases the risks of being caught and penalized for internet abuses, which, from an instrumental point of view, is likely to drive employees towards compliance with the IUP. Therefore,

H1: Perceived certainty of sanction has a positive impact on IUP compliance intention.

Besides sanction certainty, a certain level of sanction severity is a necessary deterrent to ensure compliance with organizational policies. Sanction severity stands for the magnitude of the cost to potential offenders if they are caught performing deviant behaviours and, therefore, is expected to reduce the appeal of deviant behaviours. A high level of perceived sanction severity has been found to reduce the misuse of IS resources (D'Arcy *et al*., 2009) and increase the compliance with general security policies (Herath & Rao, 2009a). Similarly, in the context of IUP compliance, when employees perceive a severe level of punishment for internet abuses, they are expected to have a high IUP compliance intention. Therefore,

H2: Perceived sanction severity has a positive impact on IUP compliance intention.

Personal ethics

Personal ethics, also called personal norms, refer to employees' normative beliefs about the appropriateness of behaviour (Wenzel, 2004). In the context of our study, personal ethics reflect employees' moral values and their value judgments about whether it is right or wrong to abuse internet access in the workplace. Personal ethics have been found to strongly influence one's intention to commit deviant behaviours such as corporate crimes (Paternoster & Simpson, 1996) and tax evasion (Wenzel, 2004). In the context of internet misuses, if an individual feels that it is against his or her ethics to commit internet abuses, he or she tends to judge internet abuses as wrong and to be innately motivated to comply with the IUP. Therefore,

H3: Personal ethics against internet abuses have a positive impact on IUP compliance intention.

Organizational justice

Justice has been widely examined in the organizational behavioural literature (Cohen-Charash & Spector, 2001). The views regarding the dimensions of justice have been evolving over time since the initial conceptualization as distributive justice by Adams (1965). Later, the content domain of justice was further expanded to include fairness perceptions of both distribution outcomes and procedures, namely distributive and procedural justice (Thibaut & Walker, 1975). Then, Bies & Moag (1986) identified interactional justice as a third dimension of organization justice that measures an individual's justice perception about the interpersonal treatment one receives as procedures are enforced. Perceptions of interactional justice are enhanced when employees are treated with respect and sensitivity and receive thorough explanations about the rationale underlying decisions made by authority. Interactional justice, however, is suggested to be more accurately broken down into two distinct dimensions, i.e. interpersonal and informational justice (Greenberg, 1993). Interpersonal justice centers on the level of respect one receives, whereas informational justice concerns the explanation about decision rationales. Colquitt (2001) empirically compared the four-dimension structure (procedural, distributive, interpersonal and informational justice) with the two-dimension and three-dimension structures and found that organizational justice is best conceptualized as four distinct dimensions. Turel *et al*. (2008) applied the four-dimension structure and verified the existence of four distinct dimensions and their differential effects on intention to reuse e-customer service. Therefore, in this study, we will examine all four justice dimensions to achieve a fine-grained examination of the role of organizational justice in IUP compliance.

Procedural justice relates to the perceived fairness of processes or procedures used to achieve the outcome (Colquitt, 2001). Different criteria have been proposed to define procedural justice (Thibaut & Walker, 1975; Leventhal, 1980; Leventhal *et al*., 1980). For example, Thibaut & Walker (1975) suggested two criteria in a legal setting, including process control (i.e. the ability to have a voice in the decision-making process) and decision control (i.e. the ability to influence the outcome). In a general setting, Leventhal (1980) identified six criteria for a procedure to be perceived as fair, including consistency, bias suppression, accuracy of information in decision-making, correctability, representativeness and ethicality (i.e. conformity to personal ethical or moral values). Prior studies have used different combinations of the former fairness criteria to examine procedural justice. Wiesenfeld *et al*. (2007), e.g. included bias suppression, accuracy and overall fairness as the defining criteria for the perceived fairness of organizational restructuring processes. Sindhav *et al*. (2006) integrated consistency, suppression of bias and overall design fairness to define passengers' fairness perception of airport security procedures. In this study, we focus on the perceived fairness of security procedures used for detecting and punishing internet abuses and took an approach similar to Sindhav *et al*. (2006) to describe perceived justice of IS security procedures. As such, an IS security procedure is likely to be considered fair if it is designed fairly and applied consistently to everyone and in a fair manner.

Procedural justice has been found to promote employees' willingness to follow corporate rules and policies (Kim & Mauborgne, 1993; Colquitt, 2001; Tyler *et al*., 2007). Employees are more willing to follow organizational rules and policies if organizations rely on fair procedures to exercise their authority. Procedural justice is important for IUP compliance as employees could

use procedural justice to assess whether they are held in high esteem when authorities develop and implement the IUP. Those who perceive a high level of procedural justice are expected to be more willing to follow the IUP.

H4: Procedural justice has a positive impact on IUP compliance intention.

Distributive justice focuses on the fairness of outcomes. It has been operationalized in many different ways in prior literature (see Sindhav *et al*., 2006). Adams (1965) argued in his equity theory that justice perceptions about distribution are formed through individuals' comparison of their own outcome-to-input ratio with the ratio of comparative others (e.g. colleagues). Feelings of inequity result when "the normative expectations of the person making social comparisons are violated, when he finds that his outcomes and inputs are not in balance in relation to those of others" (Adams, 1965, p. 280). Studies have also identified other standards to determine distributive justice (Colquitt, 2001). For example, Leventhal (1976) proposed a different conceptualization of equity standard and suggested that equity occurs when an individual's rewards/benefits are commensurate with his or her contributions. In other words, an individual will perceive an outcome to be fair if the benefits of the outcome are commensurate with his or her inputs or costs. Leventhal's equity standard has been applied in other commonly used measures in the justice literature (Sweeney & McFarlin, 1993; Colquitt, 2001). In line with the widely adopted measure proposed by Colquitt (2001), we applied the equity standard by Leventhal (1976) in this study. In the context of IUP compliance, distributive justice occurs when employees believe that restricting personal internet use at the workplace (their inputs) could lead to a commensurate level of benefits such as increased security, productivity and improved job performance. So, those perceiving a high level of distributive justice in following the IUP would be more willing to bear the costs such as the inconvenience or other losses from restricting their personal internet usage. Therefore, we have

H5: Distributive justice has a positive impact on IUP compliance intention.

Procedural justice and distributive justice have also been suggested to influence compliance with organizational policies indirectly through shaping employee's value judgement (Tyler *et al*., 2007). They may influence employees' views about the legitimacy of corporate policies and congruency with their own values (Tyler *et al*., 2007). For IUP compliance, fair procedures and outcomes are expected to increase the value congruence between an individual employee and the organization. Employees are more likely to adjust their own value judgment about internet misuses in line with the values of the organization. Such increased value congruence will drive employees to form stronger level of personal ethical objections against internet abuses. Therefore,

H6: Procedural justice has a positive impact on personal ethics against internet abuses.

H7: Distributive justice has a positive impact on personal ethics against internet abuses.

Interpersonal justice focuses on the conduct of those who enforce the procedures, such as whether they are respectful and polite to those affected by the procedures (Wenzel, 2005). Interpersonal justice has been suggested to increase individuals' intention to support the decisions of authorities (Greenberg, 1993; Tyler & Huo, 2002). For example, pay cut decisions were

accompanied by lower rates of company theft and turnover when they were explained in details and in a respectful way (Greenberg, 1993). Taxpayers were found to be more compliant with tax laws when they felt they were treated fairly and respectfully by the tax authority (Wenzel, 2006). In the context of IUP compliance, interpersonal justice is conceptualized as perceived fairness of the interpersonal treatment by those enforcing security policies. In line with these prior legal and organizational studies, employees are expected to be more inclined to comply with IUP when they perceive fair treatment from those enforcing security policies. At the same time, interpersonal justice may also influence IUP compliance intention indirectly through personal ethics. Respectful and polite treatment recognizes an employee's status and membership in the organization (Tyler, 1997), which could drive the employee to align his or her value judgment with the values of the organization and increase his or her personal ethics concerning internet misuse at the workplace. Therefore,

H8: Interpersonal justice has a positive impact on IUP compliance intention.

H9: Interpersonal justice has a positive impact on personal ethics against internet abuses.

Informational justice emphasizes the principle that authorities should share sufficient information on the process and outcome with those affected by their decisions (Sindhav *et al*., 2006). Employees were found to better comply with a corporate smoking ban when they were supplied with detailed information about the reasons of the smoking ban (Greenberg, 1994). In the context of taxation, tax letters reflecting the principle of informational justice were suggested to increase taxpayers' compliance with tax laws (Wenzel, 2006). For IUP compliance, informational justice arises when the organization is perceived open in communicating why an IUP is necessary and what procedures have been deployed for detecting and punishing internet abuses. Employees should be more willing to comply with IUP when they perceive information fairness in the communication of IUP by the organization. Besides the direct impact on IUP compliance intention, such information sharing about IUP also helps to engender a sense of belonging to the organization and drives one to align one's innate desires with the need of the organization, i.e. IUP enforcement. So, a high level of informational justice may also indirectly increase IUP compliance intention through elevating personal ethical objections against internet abuses. Therefore,

H10: Informational justice has a positive impact on IUP compliance intention.

H11: Informational justice has a positive impact on personal ethics against internet abuses.

Control variables

In this study, we also controlled four variables that might influence employees' intention to comply with IUP: gender, age, internet experience and the existence of internet monitoring practices in the company. Women have been shown to be more inclined to follow information security policies (Herath & Rao, 2009a). Internet experience has been found to increase one's IUP compliance intention (Li *et al*., 2010). The awareness of internet monitoring practices is also likely to increase one's intention to comply with the IUP.

METHODOLOGY

Variable measurement

To increase measurement reliability, most of the constructs were measured using pre-existing instruments from prior research with slight rewording where needed for our research context, i.e. IUP compliance. Sanction certainty and sanction severity were measured using items from Peace *et al*. (2003). Personal ethics measures were modifications of those developed by Wenzel (2004). The four organizational justice dimensions, i.e. procedural, distributive, interpersonal and informational justice, were adapted from the studies by Colquitt (2001) and Sindhav *et al*. (2006). IUP compliance intention was measured using scales developed by Limayem *et al*. (1999) and Peace *et al*. (2003). All these scales were operationalized as reflective ones and measured using five-point scales. The detailed measures for each construct are available in the Appendix.

Study design, procedure and participants

Organizational employees who are regulated by their companies' IUP represent the target population of this study. The research model was tested on employees in the USA by using an online survey. Potential respondents were selected from a random sample of Zoomerang's database. Zoomerang.com, a leading online survey administration and management company, has taken great effort to maintain the reliability, accuracy and quality of their data. Advanced technologies are adopted to ensure that each respondent is real, unique and engaged. Point systems and related rewards serve as incentives for survey participation. All participants in this survey were contacted through Zoomerang.com and stayed anonymous to researchers. The front page of our online survey gave the informed consent to potential survey respondents, informing them of the purpose of the study and the voluntary nature of their participation. On the second survey page, they were requested to answer two filter questions about whether they use the internet in the workplace and whether they are aware of any internet use policies implemented in their organization. As we are interested in factors motivating employees to follow the IUP of their organization, only those who answered 'Yes' to both filter questions could proceed to answer the rest of the questions in the online survey.

We collected a total of 241 valid responses. The respondents work in different roles including managerial, professional, technical, sales and clerical. As shown in Table 1, their age is mostly in the range of 20–49 years old. 56% of them are men and 44% are women. Most of them have used the internet for 6 or more years. The distribution of firm sizes shows a reasonable coverage of small, medium-sized and large firms. All these suggest that our sample is quite heterogeneous, which increases the external validity of our study.

DATA ANALYSIS

We used partial least squares (PLS) to analyse the measurement model and test the research hypotheses. PLS, as a component-based structural equation modelling approach, places minimal restrictions on sample size (Chin *et al*., 2003). PLS also does not assume a multivariate normal distribution and interval scales (Wold, 1982). To evaluate the appropriateness of PLS for our

Table 1. Demographic characteristics

Employee characteristics						Firm size (no. of employees)	
Gender		Age (Year)		Internet exp. (Year)			
Male	56%	<20	1%	<1	<1%	1–10	3%
Female	44%	20–29	29%	1–5	3%	11–250	21%
		30–39	25%	6–10	35%	251–500	15%
		40–49	19%	11–15	37%	501–1000	12%
		50 +	26%	>15	25%	1001–5000	18%
						5000 +	31%

data analysis, we performed Shapiro–Wilk test to check the normality of all measurement items and found that they all significantly depart from normal distribution. In addition, our research model consists of two binary control variables, i.e. gender and the existence of internet monitoring practices. Therefore, we used PLS instead of other SEM techniques. Statistical significance testing was performed using 200 bootstrap samples with each sample consisting of 241 cases.

Measurement model

Before testing the research model, we first assessed the measurement quality of all scales based on their convergent validity, reliability and discriminant validity. Convergent validity is suggested if factor loadings are 0.60 or higher and each item loads significantly on its latent construct (Gefen & Straub, 2005). All items load significantly (p-value < 0.001) on their corresponding latent construct with loading values above 0.60 (Table 2), indicating sound convergent validity of our measurement model. Reliability was assessed using composite reliability and average variance extracted (AVE). All scales were found to be reliable as all their composite reliability values are above 0.7 threshold and AVE above 0.5 threshold recommended by Bagozzi & Yi (1988). To check discriminant validity, we examined both the loading and cross-loading matrix (Table 2) and the correlation matrix (Table 3). In the loading and cross-loading matrix, all measurement items should load higher on their respective construct than on other constructs. Second, in the correlation matrix, the square root of the AVE of each construct should be much higher than the interconstruct correlations, i.e. the correlations between that construct and any other constructs (Fornell & Larcker, 1981). From Tables 2 and 3, all latent constructs satisfy these two criteria for discriminant validity. Therefore, our measurement model exhibits sound reliability and validity necessary for further testing of our research hypotheses.

As with other cross-sectional studies that measure independent and dependent variables using the same survey over the same set of subjects, common method variance (CMV) may be a source of biases influencing the results of our study. To test the degree of CMV, we first performed Harmon's single-factor test (Podsakoff *et al*., 2003), in which all measurement items of those latent constructs were loaded into a principal component factor analysis. The unrotated factor solution consisted of six factors with the first factor accounting for 36% of the variance. Therefore, no single factor could explain the majority of the variance, suggesting that the data set does not have substantial amount of CMV. We then applied the marker-variable technique

Table 2. Loadings, composite reliability (CR) and average variance extracted (AVE) of measurement instruments

		Loadings and cross-loadings							
Constructs/items		1	2	3	4	5	6	7	8
1. SanCert	SanCert1	**0.90****	0.52	0.14	0.25	0.16	0.20	0.18	0.22
CR = 0.91	SanCert2	**0.94****	0.48	0.20	0.31	0.27	0.24	0.26	0.28
AVE = 0.84									
2. SanSev	SanSev1	0.46	**0.91****	0.30	0.23	0.22	0.01	0.19	0.18
CR = 0.91	SanSev2	0.53	**0.92****	0.26	0.28	0.25	0.11	0.17	0.19
AVE = 0.84									
3.PerEth	PerEth1	0.20	0.36	**0.80****	0.32	0.42	0.21	0.33	0.34
CR = 0.83	PerEth2	0.05	0.17	**0.86****	0.17	0.32	0.12	0.31	0.29
AVE = 0.62	PerEth3	0.19	0.17	**0.69****	0.21	0.31	0.15	0.28	0.28
4. ProJus	ProJus1	0.30	0.31	0.28	**0.91****	0.38	0.44	0.46	0.36
CR = 0.94	ProJus2	0.27	0.25	0.27	**0.95****	0.39	0.54	0.51	0.35
AVE = 0.84	ProJus3	0.27	0.21	0.28	**0.88****	0.44	0.58	0.58	0.33
5. DisJus	DisJus1	0.31	0.24	0.33	0.38	**0.86****	0.23	0.42	0.45
CR = 0.91	DisJus2	0.16	0.21	0.43	0.42	**0.92****	0.27	0.46	0.44
AVE = 0.78	DisJus3	0.19	0.23	0.43	0.37	**0.86****	0.19	0.42	0.40
6. IntJus	IntJus1	0.23	0.03	0.21	0.56	0.26	**0.96****	0.58	0.24
CR = 0.98	IntJus2	0.25	0.07	0.20	0.54	0.25	**0.98****	0.60	0.25
AVE = 0.93	IntJus3	0.23	0.09	0.19	0.54	0.25	**0.95****	0.58	0.24
7. InfJus	InfJus1	0.18	0.11	0.34	0.49	0.41	0.57	**0.87****	0.32
CR = 0.92	InfJus2	0.22	0.24	0.35	0.48	0.44	0.51	**0.90****	0.31
AVE = 0.80	InfJus3	0.25	0.17	0.37	0.53	0.46	0.55	**0.91****	0.38
8. Intent	Intent1	0.20	0.14	0.28	0.23	0.41	0.19	0.24	**0.83****
CR = 0.93	Intent2	0.29	0.22	0.38	0.37	0.45	0.22	0.36	**0.95****
AVE = 0.82	Intent3	0.24	0.18	0.38	0.40	0.46	0.26	0.42	**0.93****

SanCert, sanction certainty; SanSev, sanction severity; PerEth, personal ethics; ProJus, procedure justice; DisJus, distributive justice; IntJus, Interpersonal Justice; InfJus, informational justice; Intent, intention to comply with internet use policy.
**$p < 0.01$.

suggested by Lindell & Whitney (2001) to estimate the magnitude of CMV and its impact on correlation coefficients among those latent constructs. Following the suggestion by Lindell & Whitney (2001), we used the second smallest positive correlation among the manifest variables as a more conservative estimate of the influence of CMV (or r_m), which was found to be 0.017. CMV-adjusted correlations among those latent constructs were then computed by partialing out r_m from the uncorrected correlations. The CMV-adjusted correlations were only slightly lower than the unadjusted correlations and their significance levels all remain the same, suggesting that CMV is not an issue of concern for our data set.

Hypothesis testing

Results of the hypothesis testing are summarized in Figure 2. Completely standardized path coefficients are displayed on each path in Figure 2. The model could explain 34% of the variance in IUP compliance intention and 25% in personal ethics.

Table 3. Discriminant validity of measurement model

Constructs	1	2	3	4	5	6	7	8
1. SanCert	**0.92**							
2. SanSev	0.54**	**0.92**						
3. PerEth	0.19**	0.30**	**0.79**					
4. ProJus	0.31**	0.28**	0.31**	**0.91**				
5. DisJus	0.24**	0.26**	0.45**	0.44**	**0.88**			
6. IntJus	0.24**	0.07	0.21**	0.57**	0.26**	**0.96**		
7. InfJus	0.24**	0.19**	0.39**	0.56**	0.49**	0.61**	**0.89**	
8. Intent	0.27**	0.20**	0.39**	0.38**	0.49**	0.25**	0.38**	**0.90**

Diagonal elements are the square root of the AVE values. Off-diagonal elements are the correlations among latent constructs.
SanCert, sanction certainty; SanSev, sanction severity; PerEth, personal ethics; ProJus, procedure justice; DisJus, distributive justice; IntJus, Interpersonal Justice; InfJus, informational justice; Intent, intention to comply with internet use policy.
**$p < 0.01$.

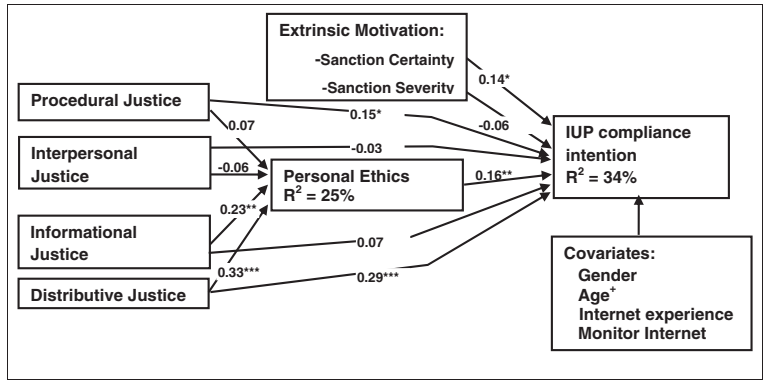

Figure 2. Results of testing hypotheses in the original research model using PLS analysis. Completely standardized estimates controlled for covariates in the research model, $^{+}p < 0.1$, $*p < 0.05$, $**p < 0.01$ and $***p < 0.001$.

For IUP compliance intention, sanction certainty was found to be significant in the hypothesized direction but sanction severity was not. Thus, the results support H1 but not H2. The research model also includes motivators for IUP compliance intention based on the self-regulatory approach, i.e. H3–H5, H8 and H10. Personal ethics, procedural justice and distributive justice were found to be significant, whereas interpersonal justice and informational justice were not. Among the four control variables, only age is marginally significant ($p < 0.1$), which is positively related to IUP compliance intention. For the formation of personal ethics against internet abuse, distributive justice and informational justice were found to be significant but procedural justice and interpersonal justice were not. Thus, the results support H7 and H11 but not H6 and H9. A summary of the hypothesis testing results is provided in table 4.

Table 4. Summary of hypothesis testing results

Hypotheses	Path coefficients	*t* value	*p*-value
H1: Sanction certainty ➔ Compliance	0.14	2.084	$p < 0.05$ (supported)
H2: Sanction severity ➔ Compliance	−0.06	0.800	$p > 0.05$ (not supported)
H3: Personal ethics ➔ Compliance	0.16	2.779	$p < 0.01$ (supported)
H4: Procedural justice ➔ Compliance	0.15	2.054	$p < 0.05$ (supported)
H5: Distributive justice ➔ Compliance	0.29	4.553	$p < 0.001$ (supported)
H6: Procedural justice ➔ Personal ethics	0.07	0.82	$p > 0.05$ (not supported)
H7: Distributive justice ➔ Personal ethics	0.33	4.021	$p < 0.001$ (supported)
H8: Interpersonal justice ➔ Compliance	−0.03	0.417	$p > 0.05$ (not supported)
H9: Interpersonal justice ➔ Personal ethics	−0.06	0.723	$p > 0.05$ (not supported)
H10: Informational justice ➔ Compliance	0.07	0.774	$p > 0.05$ (not supported)
H11: Informational justice ➔ Personal ethics	0.23	2.876	$p < 0.01$ (supported)

DISCUSSION

Key findings and limitations

We employed an integrated sanction-based command-and-control and self-regulatory model to investigate the determinants of employees' IUP compliance intention. Our study shows that employees' IUP compliance intention is motivated by self-regulatory forces, including personal ethics and organizational justice beliefs. Sanction mechanisms, although less effective than self-regulation forces, also shape IUP compliance intention. The deterrence effect of formal sanctions is largely exerted through sanction certainty rather than sanction severity. The lack of statistical significance of perceived sanction severity concurs with findings of many of the previous studies in criminology (see Paternoster, 1987; Wenzel, 2004). One possible reason may be the relatively low level of perceived sanction severity for internet abuses. In this study, the average perceived sanction severity is 2.5 on a five-point scale. That is, the consequences of sanctions relating to internet misuse were not perceived by employees to be severe.

The results of this study also suggest that organizational justice beliefs not only influence IUP compliance intention directly but also indirectly through fostering strong personal ethics against internet abuses. In particular, distributive justice was found to promote IUP compliance intention both directly and indirectly through personal ethics. Procedural justice was found to only exert direct influence on IUP compliance intention. Informational justice indirectly influences IUP compliance intention through personal ethics.

The hypothesized indirect effects of procedural justice and interpersonal justice through personal ethics were not supported in this study. The effect of procedural justice on personal ethics may be dominated by that of informational justice. Informational justice centers on the communication of IUP and related procedures for detecting and punishing internet abuses. To the extent that employees rely on information communication or the awareness of IUP to form their beliefs, informational justice could very likely serve as a more salient factor influencing one's internal personal ethical views than procedural justice. The lack of statistical significance of interpersonal justice may be attributed to the limited direct daily interaction between employees and those enforcing IS security policies, i.e. shallow relationships. Prior studies in

marketing suggest that the effect of interpersonal justice could be overridden by that of distributive justice in the existence of a shallow relationship (Hoffman & Kelley, 2000).

In addition, interpersonal justice and informational justice were not found to have significant direct impact on IUP compliance intention. Therefore, the effect of informational justice is fully mediated through personal ethics. Interpersonal justice has neither a direct nor an indirect impact on IUP compliance intention. As mentioned previously, the non-significance of interpersonal justice may be attributed to the limited direct daily interaction between employees and those enforcing IS security policies, i.e. shallow relationships.

We further compared the relative efficacy of sanction-based approach with the self-regulatory approach. Two alternative models for pure sanction-based approach and pure self-regulatory approach were built separately with the control variables to predict IUP compliance intention (Figure 3). The R^2 for the pure sanction-based model is only 12% in comparison with 32% for the pure self-regulatory model (Figure 3). The result suggests that self-regulatory approach explains more variation in IUP compliance intention than sanction-based approach. Following the self-regulatory approach, personal ethics and organizational justice beliefs are two dominant factors in explaining IUP compliance intention.

As discussed in the theoretical foundation section, sanction and organizational justice each consist of multiple dimensions. It would be interesting to build and test a third alternative model by implementing sanction and organizational justice as two second-order factors (Figure 4). In particular, we modelled them as two formative constructs as their corresponding first-order constructs have low to moderate correlations (Table 3). This is in line with the suggestion by Pavlou & Sawy (2006) that a reflective second-order factor would show extremely high correlations among its first-order factors (often above 0.8). This third model provides a more parsimonious view about the relative impact of sanction-based approach and self-regulatory approach than the other models. Again, personal ethics and organizational justice were shown to be the prevailing motivators for IUP compliance. Sanction is only marginally significant.

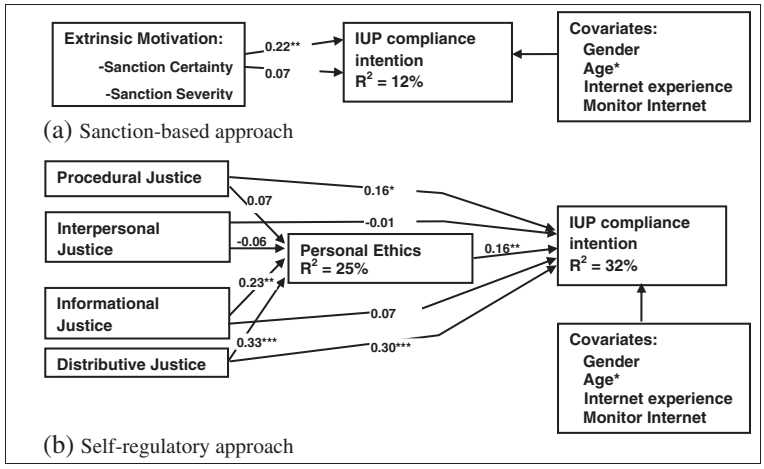

Figure 3. Results of comparing the relative efficacy of sanction-based approach and self-regulatory approach using PLS analysis. Completely standardized estimates controlled for covariates in the research model, $^*p < 0.05$, $^{**}p < 0.01$ and $^{***}p < 0.001$.

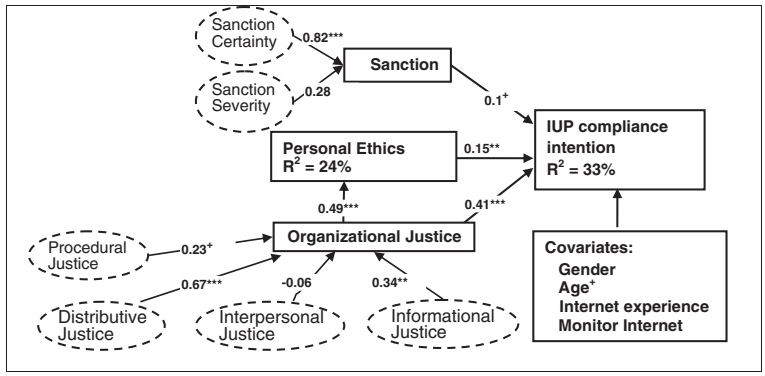

Figure 4. Results of testing the research model with sanction and organizational justice implemented as second-order constructs. First-order factors constituting the second-order factors were shown in dashed circles with their weights displayed on the paths leading to the second-order factors. Completely standardized estimates controlled for covariates in the research model, $^{+}p < 0.1$, $^{*}p < 0.05$, $^{**}p < 0.01$ and $^{***}p < 0.001$.

Akin to other behaviour-driven investigations, our study has inevitable limitations. One limitation is the use of behavioural intention as a surrogate for employees' actual compliance behavior. This is consistent with the research practice of most of the studies based on the theory of reasoned action (Fishbein & Ajzen, 1975). According to theory of reasoned action, behavioural intention is a strong predictor of actual behaviour. But future studies could be conducted to test our research model by monitoring employees' actual compliance behaviour or collecting the self-reported compliance behaviours. However, both approaches for gathering actual behaviour data face challenges that need to be handled carefully. The IUPs of many organizations allow occasional or limited personal internet use without specifying the exact amount of time permitted for personal internet use. A close collaboration with firms would be needed to not only collect the actual compliance data but also interpret whether any violation has occurred. Moreover, if the actual internet use data are to be matched with survey data measuring other constructs in the research model, the identity of survey respondents will be revealed. In this case, employees' responses to most of the survey questions will be biased to reflect what employers would expect instead of their own beliefs. Collecting self-reported compliance data incurs similar concerns for anonymity and social desirability. Individuals are unwilling to truly report their actual behaviours related to policy violation or crimes (Hu *et al*., 2011). It is critical to emphasize the anonymous nature of the survey to reduce the effect of social desirability in survey design and administration. Another limitation of our study is that we only examined internet abuses in general without differentiating specific types of internet abuses such as online shopping and cyberstalking in the workplace. The model may not be extendable to severe cybercrimes.

Contributions

This paper has four major contributions to current IS security policy compliance literature. First, the research model integrates and compares the extrinsic command-and-control approach with

the intrinsic self-regulatory approach to provide a better understanding of factors motivating IUP compliance intention. Second, the self-regulatory approach identifies some of the fundamental but often overlooked factors in understanding security policy compliance such as personal ethics and organizational justice beliefs. These self-regulatory factors shed light on inconsistent findings about formal sanctions in prior studies (Pahnila *et al*., 2007; Herath & Rao, 2009a). The effect of formal sanctions on security policy compliance may very likely be dominated by that of internal motivations of potential offenders. Formal sanctions become less of a necessity for individuals with no internal motivation to commit deviant acts. Third, this is a first study that has differentiated and empirically tested the roles of four dimensions of organizational justice in IS policy compliance. This could facilitate the development of fine-grained strategies that companies can implement to enhance the compliance with their security policies. Finally, our research model can be readily applied to other security policy compliance contexts. Although in this study, the model was empirically tested for internet abuse, the empirical support for our research model may also advance the understanding of employees' compliance with security policies in general, dealing with activities such as the access and transfer of confidential corporate data, and password security.

Implications for research

This study has several important research implications for individual compliance with security policies. First, our study found that IUP compliance intention is influenced by both command-and-control and self-regulatory approaches. The self-regulatory approach emphasizes the internal motivations of potential offenders. Examining the effect of formal sanctions without considering the role of internal motivations is not sufficient. A complete understanding of individual employees' security policy compliance must include intrinsic together with extrinsic motivational forces.

Second, our results show that the self-regulatory approach has a stronger influence over IUP compliance intention than the command-and-control approach. Voluntary compliance with IUP is more likely among employees with strong ethics against internet abuses and high perceived fairness in organizational procedures and outcomes. Currently, the effect of the self-regulatory approach on security policy compliance has only received sparse research attention (Herath & Rao, 2009a, 2009b). Future studies are needed to explore other self-regulatory factors that could motivate the voluntary compliance with security policies. For example, the judgment about the legitimacy of the organization has been suggested as another self-regulatory approach for rule adherence (Tyler, 2006; Tyler *et al*., 2007), which needs to be adapted and empirically tested in the context of security policy compliance.

Third, the study supports the significant impact of organizational justice on personal ethics. A high level of informational justice and distributive justice could help organizations enhance an employee's ethics against internet abuses. This finding suggests that one's ethical view about a specific deviant act is dynamic, i.e. malleable with the perceived fairness of organizational information practices and outcomes that one receives from avoiding the deviant act. Besides organizational justice, an employee's ethical view about the deviant act may also be molded by other factors, such as the moral beliefs of most other employees in the organization and

the existence of legal regulation. For example, the existence of laws regulating severe cybercrimes may increase an employee's ethics against internet abuses. Future studies are also necessary to explore specific methods for increasing organizational justice in enforcing security policies. For example, it is not clear whether training about the security risks of internet abuses would be effective in increasing distributive justice.

Implications for practice

Pragmatically speaking, organizations could resort to two approaches to secure compliance with the IUP. One approach would be to emphasize the probability of being caught engaging in internet abuses. Organizations would need to invest in surveillance technology or personnel to monitor the internet usage such as checking computer history and network logs. Employees should be made aware of the existence of the computer and network surveillance implemented in the organization.

Because the results of this study found that the self-regulatory approach is more effective than formal sanctions, a second promising approach would be to tap into self-regulation or employees' intrinsic motivation to comply with the IUP. This may cause employees to accept the IUP voluntarily even when they are unlikely to be caught and punished for internet abuses at the workplace. Organizations would be able to reduce the expenditure on creating and maintaining the monitoring systems and the cost of punishing deviant employees. In the long term, the self-regulatory approach also helps to boost the morale of employees as self-regulation builds on employees' internal values, leading to internalization of organization values and employee identification.

The findings of our research model shed light on several routes that could be taken to utilize employees' intrinsic motivation to achieve self-regulation. In this study, we identified several intrinsic motivators for IUP compliance, including organizational justice beliefs and personal ethics. First, organization could leverage procedural justice and distributive justice to directly influence employees' compliance intention. Organizations need to pay attention to the perceived fairness in organizational procedures and distributive outcomes. To influence employees' distributive justice belief, organizations should explicitly educate their employees about the benefits of restricting personal internet activities in the workplace by emphasizing the negative impact of internet abuses. For example, Bock & Ho (2009) empirically found the non-work-related emails and personal internet usage negatively impacted employee job performance. The annual security report of Sophos has consistently rated the internet as the most important route for security breaches over the past few years. Organizations could also try to increase the perceived fairness of organizational procedures by incorporating fairness criteria proposed in prior literature when designing and implementing IUP. For example, organizations need to implement IUP consistently across all employees.

At the same time, our analysis results support the central role of personal ethics in the self-regulatory strategy for achieving policy compliance. Therefore, another route for organizations to activate intrinsic self-regulation is through personal ethics or aligning employees' personal values with those of their organization and policies. Employees are more willing to comply with organizational policies viewed as consistent with their moral values. To

engage employees' personal ethics, organizations could rely on either organizational justice or ethical training. As suggested by the results of this study, organizations could foster favourable personal ethics by building distributive justice and informational justice. Informational justice could be established through periodical information security training or security awareness campaigns to communicate with employees about the IUP. Lastly, as suggested by Calluzzo & Cante (2004), ethics training would be necessary to help employees understand what constitute ethical or appropriate use of IT resources such as internet access at workplace.

Overall, organizations need to also rely on the self-regulatory approach in which value-based intrinsic motivations are the drivers for IUP compliance. Self-regulation has been considered effective for most people (Tyler, 2009) and extrinsic sanction-based approaches could serve as a supplementary measure. Extrinsic sanctions may be more suitable for a small group of employees whose personal moral values deviate from those of their organizations or who are unable or unwilling to act on their moral values (Tyler, 2009). These employees may be identified through questionnaires that gauge their value judgments about personal internet use at the workplace and measure their propensity to conduct deviant acts, i.e. low self-control (Gottfredson & Hirschi, 1990).

It would also be interesting to investigate individual differences. Employees' personal traits may determine that some people are highly motivated by intrinsic factors, whereas others are more motivated by extrinsic factors. One example of such personal traits could be causality orientations (Deci, 1980). Three types of causality orientations, including autonomy orientation, control orientation and impersonal orientation, correlate to different degrees of self-determination (Deci & Ryan, 1985). People with a high level of autonomy orientation are more self-determined; they tend to be more intrinsically motivated and less likely to be affected by extrinsic factors (Deci & Ryan, 1985). Future research may test the effect of employees' personal traits on the relative effectiveness of self-regulatory approach and sanction-based approach.

CONCLUSIONS

Despite its wide deployment in organizations, the IUP is not considered to be effective in reducing internet abuses in the workplace. Non-compliance with IUP imposes a great challenge for managing security as internet abuses expose companies to additional security threats from the internet. This study investigated factors that motivate employees' IUP compliance intention. Previous studies have primarily focused on extrinsic motivational forces such as formal sanctions and security threats, and have largely ignored the effect of intrinsic motivations such as personal ethics and employees' justice beliefs. As one of the early studies shedding light on both crucial approaches, this paper offers an integrative understanding of IUP compliance intention considering both extrinsic and intrinsic motivational forces. The empirical results of our study suggest the importance of the self-regulatory approach through its emphasis on internal ethical values of employees and perceived organizational justice in dealing with IUP violations.

REFERENCES

Adams, J.S. (1965) Inequity in social exchange. In: *Advances in Experimental Social Psychology*, Berkowitz, L. (ed.), pp. 267–299. Academic Press, New York.

Bagozzi, R.P. & Yi, Y. (1988) On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, **16**, 74–94.

Bies, R. & Moag, J. (1986) Interactional justice: communication criteria, In: *Research on Negotiations in Organizations*, Lewicki, R., Sheppard, B. & Bazerman, M. (eds.), pp. 43–55. JAI Press, Greenwich, CT.

Bock, G.-W. & Ho, S.L. (2009) Non-work related computing (NWRC). *Communications of the ACM*, **52**, 124–128.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. & Boss, R.W. (2009) If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems* **18**, 151–164.

Bulgurcu, B. (2010) Information security policy compliance: an empirical study of rational-based beliefs and information security awareness. *MIS Quarterly*, **34**, 523–548.

Calluzzo, V.J. & Cante, C.J. (2004) Ethics in information technology and sofware use. *Journal of Business Ethics*, **51**, 301–312.

CareerBuilder. (2012). Half of workers plan to do some online holiday shopping at work. http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=11%2F26%2F2012&id=pr726&ed=12%2F31%2F2012. Accessed June 8 2013.

Chin, W.W., Marcolin, B.L. & Newsted, P.R. (2003) 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. *Information Systems Research*, **14**, 189–217.

Cohen-Charash, Y. & Spector, P.E. (2001) The role of justice in organizations: a meta-analysis. *Organizational Behavior and Human Decision Processes*, **86**, 278–321.

Colquitt, J.A. (2001) On the dimensionality of organizational justice: a construct validation of a measure. *Journal of Applied Psychology*, **86**, 386–400.

D'Arcy, J., Hovav, A. & Galletta, D. (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, **20**, 79–98.

Deci, E.L. (1980) *The Psychology of Self-Determination*. Heath, Lexington, MA.

Deci, E.L. & Ryan, E. (1985) The general causality orientations scale: self-determination in personality. *Journal of research in personality*, **19**, 109–134.

Dhillon, G. & Torkzadeh, G. (2006) Value-focused assessment of information security in organizations. *Information Systems Journal*, **16**, 293–314.

Fishbein, M. & Ajzen, I. (1975) *Belief Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Addison-Wesley, Reading, MA.

Fornell, C. & Larcker, D. (1981) Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, **18**, 39–50.

Gefen, D. & Straub, D. (2005) A practical guide to factorial validity using PLS-graph: tutorial and annotated example. *Communications of the AIS*, **16**, 91–109.

Gottfredson, M.R. & Hirschi, T. (1990) *A General Theory of Crime*. Stanford University Press, Stanford, CA.

Greenberg, J. (1993) The social side of fairness: interpersonal and informational classes of organizational justice. In: *Justice in the Workplace: Approaching Fairness in Human Resource Management*, Cropanzano R. (ed.), pp. 79–103. Erlbaum, Hillsdale, NJ.

Greenberg, J. (1994) Using socially fair treatment to promote acceptance of a work-site smoking ban. *Journal of Applied Psychology*, **79**, 288–297.

Herath, T. & Rao, H.R. (2009a) Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, **47**.

Herath, T. & Rao, H.R. (2009b) Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems*, **18**, 106–125.

Hoffman, K.D. & Kelley, S.W. (2000) Perceived justice needs and recovery evaluation: a contingency approach. *European Journal of Marketing*, **34**, 418–432.

Hu, Q., Xu, Z., Dinev, T. & Ling, H. (2011) Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, **54**, 54–60.

Johnston, A. & Warkentin, M. (2010) Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, **34**, 549–566.

Kim, W.C. & Mauborgne, R.A. (1993) Procedural justice, attitudes, and subsidiary top management compliance with multinationals' corporate strategic decisions. *Academy of Management Journal*, **36**, 502–526.

Lau, V.C.S., Au, W.T. & Ho, J.M.C. (2003) A qualitative and quantitative review of antecedents of counterproductive behavior in organizations. *Journal of Business and Psychology*, **18**, 73–99.

Lerner, M.J. (2003) The justice motive: where social psychologists found it, how they lost it, and why they may not find it again. *Personality and Social Psychology Review*, **7**, 388–399.

Leventhal, G.S. (1976) Fairness in social relationships. In: *Contemporary Topics in Social Psychology*, Thibaut J. W., Spence J.T. & Carson R.C. (eds.), pp. 211–239. General Learning Press, Morristown, NJ.

Leventhal, G.S. (1980) What should be done with equity theory. In: *Social Exchange: Advances in Theory and Research*, Gergen K., Greenberg M. & Willis R. (eds.), pp. 27–55. Plenum, New York.

Leventhal, G.S., Karuza, J. & Fry, W. (1980) Beyond fairness; a theory of allocation preferences. In: *Justice and Social Interaction*, Mikula G. (ed.), pp. 167–218. Springer-Verlag, New York.

Li, H., Zhang, J. & Sarathy, R. (2010) Understand the compliance with the internet use policy from the perspective of rational choice theory. *Decision Support Systems*, **48**, 635–645.

Lim, V.K.G. (2002) The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior*, **23**, 675–694.

Limayem, M., Khalifa, M. & Chin, W.W. (1999) Factors motivating software piracy: a longitudinal study. *Proceedings of the International Conference on Information Systems*, pp. 124–131, North Carolina, United States.

Lindell, M.K. & Whitney, D.J. (2001) Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, **86**, 114–121.

Pahnila, S., Siponen, M. & Mahmood, A. (2007) Employees' behavior toward IS security policy compliance. *40th Hawaii International Conference on System Sciences*, IEEE Computer Society, Hawaii.

Paternoster, R. (1987) The deterrent effect of the perceived certainty and severity of punishment: a review of the evidence and issues. *Justice Quarterly*, **4**, 173–217.

Paternoster, R. & Simpson, S. (1996) Sanction threats and appeals to morality: testing a rational choice model of corporate crime. *Law & Society Review*, **30**, 549–583.

Pavlou, P.A. & Sawy, O.A.E. (2006) From IT leveraging competence to competitive advantage in turbulent environments: the case of new product development. *Information Systems Research*, **17**, 198–227.

Peace, A.G., Galletta, D. & Thong, J. (2003) Software piracy in the workplace: a model and empirical test. *Journal of Management Information Systems*, **20**, 153–177.

Pee, L.G., Woon, I.M.Y. & Kankanhalli, A. (2008) Explaining non-work-related computing in the workplace: a comparison of alternative models. *Information & Management*, **45**, 120–130.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y. & Podsakoff, N.P. (2003) Common method biases in behavior research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, **88**, 879–903.

Schweitzer, D. (2004). Workplace Web use: give 'em an inch.... http://www.searchsap.techtarget.com/news/article/0,289142,sid21_gci1009417,00.html#. Accessed February 15 2009.

Sindhav, B., Holland, J., Rodie, A.R., Adidam, P.T. & Pol, L.G. (2006) The impact of perceived fairness on satisfaction: Are airport security measures fair? Does it matter? *Journal of Marketing Theory and Practice*, **14**, 323–335.

Siponen, M. & Vance, A. (2010) Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, **34**, 487–502.

Son, J.-Y. (2011) Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, **48**, 296–302.

Sophos. (2009). Sophos security threat report. https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophossecuritythreatreportjul2009nawpus.pdf. Accessed February 11 2014.

Straub, D.W. (1990) Effective IS security: an empirical study. *Information Systems Research*, **1**, 255–276.

Sweeney, P.D. & McFarlin, D.B. (1993) Workers' Evaluations of the "ends" and "means": an examination of four models of distributive and procedural justice. *Organizational Behavior and Human Decision Processes*, **55**, 23–40.

Thibaut, J. & Walker, L. (1975) *Procedural Justice: A Psychological Analysis*. Lawrence Erlbaum, Hillsdale, NJ.

Turel, O., Yuan, Y. & Connelly, C.E. (2008) In justice we trust: predicting user acceptance of e-commerce service. *Journal of Management Information Systems*, **24**, 123–151.

Tyler, T.R. (1997) The psychology of legitimacy: a relational perspective on voluntary deference to authorities. *Personality and Social Psychology Review*, **1**, 323–345.

Tyler, T.R. (2006) Restorative justice and procedural justice: dealing with rule breaking. *Journal of Social Issues*, **62**, 307–326.

Tyler, T.R. (2009) Legitimacy and criminal justice: the benefits of self-regulation. *Ohio State Journal of Criminal Law*, **7**, 307–359.

Tyler, T.R. & Huo, Y.J. (2002) *Trust in the Law: Encouraging Public Cooperation with the Police and Courts*. Russell Sage Foundation, New York.

Tyler, T.R., Callahan, P.E. & Frost, J. (2007) Armed, and dangerous (?): motivating rule adherence among agents of social control. *Law & Society Review*, **41**, 457–492.

Ugrin, J.C. & Pearson, J.M. (2013) The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior*, **29**, 812–820.

Vance, A. & Siponen, M.T. (2012) IS security violations: a rational choice perspective. *Journal of Organizational and End User Computing*, **24**, 21–41.

Webroot. (2010). Webroot research shows half of SMBs block employee access to Facebook. http://www.webroot.com/En_US/pr/web-security/ent/research-shows-half-of-smbs-block-employee-access-to-facebook-111510.html. Accessed June 8 2013.

Wenzel, M. (2002) The impact of outcome orientation and justice concerns on tax compliance: the role of taxpayers' identity. *Journal of Applied Psychology*, **87**, 629–645.

Wenzel, M. (2004) The social side of sanctions: personal and social norms as moderators of deterrence. *Law and Human Behavior*, **28**, 547–567.

Wenzel, M. (2005) Motivation or rationalization? Causal relations between ethics, norms and tax compliance. *Journal of Economic Psychology*, **26**, 491–508.

Wenzel, M. (2006) A letter from the tax office: compliance effects of informational and interpersonal justice. *Social Justice Research*, **19**, 345–357.

Wiesenfeld, B.M., Swann, W.B., Brockner, J. & Bartel, C. (2007) Is more fairness always preferred? Self-esteem moderates reactions to procedural justice. *Academy of Management Journal*, **50**, 1235–1253.

Willison, R. & Warkentin, M. (2013) Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly*, **37**, 1–20.

Wold, H. (1982) Soft modeling: the basic design and some extensions. In: *Systems Under Indirect Observation: Causality, Structure, Prediction*, Joreskog K.G. & Wold H. (eds.), pp. 1–47. North-Holland, Amsterdam.

Young, K.S. & Case, C.J. (2004) Internet abuse in the workplace: new trends in risk management. *Cyberpsychology & Behavior*, **7**, 105–111.

APPENDIX: SURVEY INSTRUMENT

Sanction Certainty (Peace *et al*., 2003)	
DetPro1	If I used the Internet access provided by the organization for non-work- related purposes, … the probability that I would be caught is (Very Low/Very High)
DetPro2	I would probably be caught. (Strongly Agree/Strongly Disagree)
Sanction Severity (Peace *et al*., 2003)	
SanSev1	If I were caught using the Internet access provided by the organization for non-work-related purposes, …I think the punishment would be (Very Low/Very High)
SanSev2	I would be severely punished by my organization. (Strongly Agree/Strongly Disagree)
Personal Ethics (Wenzel, 2004) (Strongly Agree/Strongly Disagree)	
PerEth1	I think I should not use the Internet access provided by the organization for non-work-related purposes.
PerEth2	To me, it is acceptable to use the Internet access provided by the organization for non-work-related purposes.
PerEth3	To me, using the Internet access provided by the organization for non-work-related purposes is a trivial offence.
Procedural Justice (Colquitt, 2001; Sindhav *et al*., 2006) (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.
Distributive Justice (Colquitt, 2001; Sindhav *et al*., 2006) (Strongly Agree/Strongly Disagree)	
DisJus1	The increase in the security of my computer and data is worth the inconvenience or other loss that I may suffer from restricting non-work-related Internet usage.
DisJus2	The increase in my productivity is worth the inconvenience or other loss that I may suffer from restricting non-work-related Internet usage.
DisJus3	The potential improvement in my performance evaluation is likely to compensate for the inconvenience or other loss that I may suffer from restricting non-work-related Internet usage.

(Continues)

APPENDIX: (Continued)

Interpersonal Justice (Colquitt, 2001; Sindhav *et al.*, 2006) (Strongly Agree/Strongly Disagree)

IntJus1	The personnel enforcing information security treated me with respect in my organization.
IntJus2	The personnel enforcing information security treated me with courtesy in my organization.
IntJus3	The personnel enforcing information security acted professionally in my organization.

Informational Justice (Colquitt, 2001; Sindhav *et al.*, 2006) (Strongly Agree/Strongly Disagree)

InfJus1	My organization has been open in communication with employees about the Internet use policy for non-work-related Internet usage.
InfJus2	Employees have been made aware of the security procedures for detecting and punishing non-work-related Internet usage.
InfJus3	My organization has a reasonable explanation about why it is necessary to enforce the Internet use policy for non-work-related Internet usage.

Intention to Comply with the Internet Use Policy (Limayem *et al.*, 1999; Peace *et al.*, 2003) (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.