Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2010 Proceedings

International Conference on Information Systems (ICIS)

2010

Understanding Compliance with Internet Use Policy: An Integrative Model Based on Command-and- Control and Self-Regulatory Approaches

Han Li
Minnesota State University Moorhead, li@mnstate.edu

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

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

Understanding Compliance with Internet Use Policy: An Integrative Model Based on Command-and-Control and Self-Regulatory Approaches

Completed Research Paper

Han Li
Minnesota State University Moorhead
Moorhead, MN 56563
li@mnstate.edu

Rathindra Sarathy
Oklahoma State University
Stillwater, OK 74078
rathin.sarathy@okstate.edu

Jie Zhang
Midwestern State University
Wichita Falls, Texas 76308
jie.zhang@mwsu.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 the compliance with security policies have largely ignored the impact of intrinsic motivations on employees' compliance intention. This paper proposes a theoretical model that integrates an extrinsic sanction-based command-and-control approach with an intrinsic self-regulatory approach to examine employees' IUP compliance intention. The self-regulatory approach centers on the effect of organizational justice and personal moral beliefs 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. Organizational justice not only influences IUP compliance intention directly, but also indirectly through fostering favorable personal moral beliefs against Internet abuses.

Keywords: Internet abuses, Internet use policy, Deterrence, Self-regulation, Organizational Justice

Introduction

The Internet is becoming the de facto platform for the cost-effective transmission of business data within the same company or among business partners. At the same time, 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 web sites. A recent Gallup poll shows that the average employee spends over 75 minutes 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 data leakages. The web is "the major vehicle for cybercriminals looking to infect computers around the world" (Sophos 2009). There is a new infected webpage every 3.6 seconds or 23,500 web pages every day. These infected webpages often appear legitimate and are exploited by hackers to spread malwares.

Most companies include an Internet use policy (IUP) as an important part of their security policy to combat Internet misuse at the work place (Young et al. 2004). However, IUPs are generally considered to be ineffective for reducing Internet misuse in most of the companies (Young et al. 2004). This highlights the importance of understanding factors influencing compliance with the IUP. This paper examines how to motivate compliance with the IUP. Prior studies have primarily focused on fear-based mechanisms to understand compliance with IS security policies (Li et al. 2010b). In this study, we compare two approaches for achieving compliance: an extrinsic sanction-based approach and an intrinsic self-regulatory approach that considers organizational justice and personal moral values, with an emphasis on the latter approach.

The remainder of the document is structured as follows: in the following section, we review the literature to identify gaps in the literature and apply deterrence theory and organizational justice theory to gain a better understanding of the IUP compliance decision. 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, and future research directions avenues.

Literature Review and Theoretical Foundation

Prior Research in Individual Security Policy Compliance

The prevalence of personal Internet usage in the workplace has attracted a lot of research. The literature has examined the impact of non-work-related computing on job performance (Bock et al. 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 strategy. However, research in the area of information security policy compliance is still in an embryonic stage (Herath et al. 2009a). Current studies on compliance with security policies are mostly based on general deterrence theory and/or protection motivation theory. They 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 (Herath et al. 2009a; Herath et al. 2009b; Pahnila et al. 2007; Siponen et al. 2006). These fear-based motivational forces are extrinsic and often considered less effective for rule adherence than self-regulatory approaches. 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 moral beliefs or act in the best interest of their organization to which they are strongly committed. Thus far, intrinsic motivation has only received sparse research attention in IS security studies. Herath and Rao (2009a) empirically tested the perceived effectiveness of one's security behavior as an intrinsic motivator for security policy compliance. Li et al (2010b) suggest that personal moral beliefs against Internet abuses are a major intrinsic motivational force influencing IUP compliance.

Prior studies have provided valuable insights as to why non-compliance with security policies occurs. However, there still exists a lack of understanding about the self-regulatory approach. It is not clear how organization 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 organizations could be used 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 and, at the same, put it in the context of organizational justice to have an in-depth understanding about the self-regulatory approach. In the subsections below, we first give an overview of extrinsic command-and-control and intrinsic self-regulatory approaches. Then, we discuss the role of organizational justice in driving self-regulatory approach.

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 behaviors. The risks from formal sanctions influence employees' decisions relating to organizational deviant behaviors (Paternoster 1987), by increasing the cost of such behaviors. 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. Rule adherence is considered to arise from an individual's intrinsic desires or feelings of personal obligation to an organization (Tyler et al. 2007). 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). Compliance could be motivated through the congruence between organizational policies and employee's moral values (Paternoster et al. 1996). In the context of IUP compliance, personal moral beliefs against Internet abuses are a type of value judgments reflecting whether restricting personal Internet use using the IUP is in line with one's moral values. In this study, we are interested in how employees' moral values on the personal use of the Internet at the workplace (personal moral beliefs against Internet abuses), are formed from the perspective of organizational justice and how personal moral beliefs together with organizational justice motivate compliance with the IUP.

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.

IUP Compliance and Organizational Justice

Internet abuses in the workplace occur in specific organizational settings. As suggested in prior studies, organizational characteristics may influence IS misuse intention (D'Arcy et al. 2009). Therefore, besides external and internal motivational forces, it is also necessary to examine organizational characteristics or the setting in which the IUP is enforced. Organizational justice is one such characteristic that has been suggested as a factor in shaping rule compliance (Tyler et al. 2007). Organizational justice is a set of fairness perceptions about 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 et al. 2001). Employees are more likely to form a favorable value judgment about organizational polices and comply with them if they perceive a high level of justice in the process and outcomes of implementing organization policies.

From the above we can conclude that deviant behaviors and security policy compliance are driven by both extrinsic and intrinsic motivational forces, i.e. formal sanctions and personal moral beliefs. Justice, as an important organizational characteristic, also influences moral beliefs and compliance with the IUP.

Research Model

In this section, we propose the research framework (Figure 1) and hypothesize the relationships among constructs. IUP compliance is modeled as the joint influence of formal sanctions and justice-based self-regulatory approach. The research model suggests that employees' IUP compliance intention will increase when 1) employees perceive high threats from formal sanctions, 2) employees have high personal moral beliefs against Internet abuses, and 3) employees perceive higher level of fairness in the procedure and outcomes of IUP policy enforcement. The model also suggests that organizational justice could enhance compliance with the IUP indirectly through shaping personal moral beliefs against Internet abuses. The following subsections illustrate each of the motivational forces and their impact on IUP compliance intention in more details.

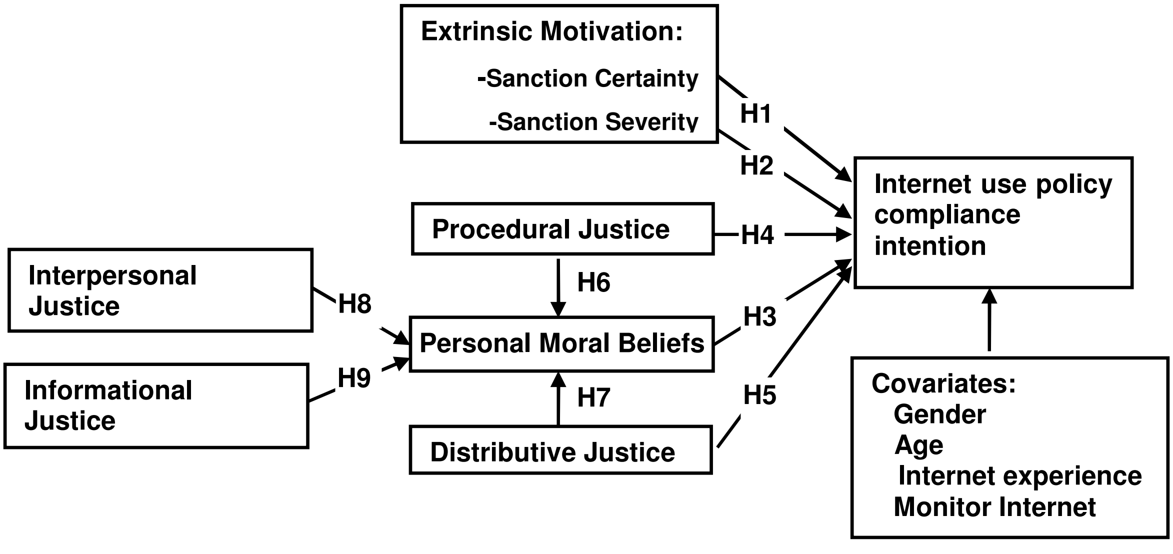

Figure 1. Research Model

Formal Sanctions

Formal sanctions or punishments have been widely studied using deterrence theory to combat individual deviant behaviors in various settings such as tax compliance , street crime, and corporate offense (Paternoster et al. 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. Deterrence has been supported as a useful strategy for reducing computer abuses and software piracy in organizations (Peace et al. 2003; Straub 1990). 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 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 certainty of sanction is employees' perception of the probability that they will be caught if they use the Internet access provided by the organization for personal purposes. High sanction certainty clearly increases the risks of Internet abuses, which, from an instrumental point of view, is likely to drive employees toward compliance with the IUP. Therefore,

H_1: Perceived certainty of sanction has a positive impact on IUP compliance intention.

Sanction severity stands for the degree of cost to potential offenders if they are caught performing deviant behaviors and, therefore, is expected to reduce the appeal of conducting deviant behaviors. 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 et al. 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,

H_2: Perceived sanction severity has a positive impact on IUP compliance intention.

Personal Moral Beliefs

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

H_3: Personal moral beliefs against Internet abuses have a positive impact on IUP compliance intention.

Organizational Justice

Organization justice consists of multiple dimensions. It was initially conceptualized as having two dimensions, namely procedural and distributive justice. Bies and Moag (1986) identified interactional justice as a third dimension of organization justice to tap an individual's justice perception about the interpersonal treatment one receives as procedures are enforced. Interactional justice is engendered when employees are treated with respect and sensitivity and receive thorough explanation 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 information justice (Greenberg 1993). Interpersonal justice centers on the level of respect one receives while information 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 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). A process is likely to be considered fair if it is designed fairly and applied consistently to everyone and in a fair manner (Sindhav et al. 2006). Procedural justice has been found to promote employees' willingness to follow corporate rules and policies (Colquitt 2001; Kim et al. 1993; 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.

H_4: 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). In this study, we use the one based on equity, which emphasizes commensuration of one's outcome with his or her inputs or costs (Sindhav et al. 2006). An individual will perceive an outcome to be fair if the benefits of the outcome are commensurate with his or her inputs or costs. 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 loss from restricting their personal Internet usage. Therefore, we have

H_5: 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 activating internal motivations, i.e. shaping employee's value judgment (Tyler et al. 2007). They may influence employees' views about the legitimacy of corporate policies and congruency with their own moral 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 moral beliefs against Internet abuses. Therefore,

H_6: Procedural justice has a positive impact on personal moral beliefs against Internet abuses.

H_7: Distributive justice has a positive impact on personal moral beliefs 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). In the context of IUP compliance, interpersonal justice is conceptualized as perceived fairness of the interpersonal treatment by those enforcing security policies. 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,

H_8: Interpersonal justice has a positive impact on personal moral beliefs against Internet abuses.

Informational justice refers to the principle that authorities should share with those affected by their decisions sufficient information on the process and outcome (Sindhav et al. 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. Such information sharing 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. In words, a high level of informational justice may foster a high level of personal moral belief against Internet abuses. Therefore,

H_9: Informational justice has a positive impact on personal moral beliefs against Internet abuses.

Control Variables

In this study, we also controlled for 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. Females have been shown to be more inclined to follow information security policies (Herath et al. 2009a). Internet experience has been found to increase one's IUP compliance intention (Li et al. 2010a). 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[1]. . Sanction certainty, and sanction severity were measured using items from Peace et al. (2003). Personal moral beliefs was modified after 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' Internet Use Policy represent the target population of this study. The research model was tested on employees in United States 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. They were first 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.

[1] A copy of the study's instrument is available from the authors on request.

Their age is in the range of 30-49 years (Table 1). 56% of them are male and 44% are female. 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. Therefore, our sample is quite heterogeneous, which increases the external validity of our study.

Table 1. Demographic Characteristics

Employee Characteristics			Firm Size
Gender	Age (Year)	Internet Exp. (Year)	(# Employees)
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%	501-1,000 12%
	50 + 26%	>15 25%	1,001-5,000 18%
			5,000+ 31%

Data Analysis

We used PLS to analyze the measurement model and test the research hypotheses. PLS, as a component-based approach, places minimal restrictions on sample size and residual distributions (Chin et al. 2003). Statistical significance testing was performed by using 100 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 et al. 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 (CR) and average variance extracted (AVE). All scales were found to be reliable as all their CR values are above 0.7 threshold and AVE above 0.5 threshold recommended by Bagozzi et al. (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 inter-construct correlations, i.e. the correlations between that construct and any other constructs (Fornell et al. 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 all cross-sectional studies, 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. 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 percent of the variance in IUP compliance intention, and 25 percent in personal moral beliefs.

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 three other motivators for IUP compliance intention based on the self-regulatory approach, i.e. H3, H4 and H5. All of them were found to be significant. Among the four control variables, only age is significant (p<0.05), which is positively related to IUP compliance intention.

For the formation of personal moral beliefs 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 H9 but not H6 and H8.

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

Constructs/Items		1	2	3	4	5	6	7	8
1. SancPro	DetPro1	**0.90**	0.52	0.14	0.25	0.16	0.20	0.18	0.22
CR = 0.91	DetPro2	**0.94**	0.48	0.20	0.31	0.27	0.24	0.26	0.28
AVE = 0.84									
2. SanSev	SanSev1	0.47	**0.90**	0.30	0.23	0.22	0.01	0.19	0.18
CR = 0.91	SanSev2	0.53	**0.93**	0.26	0.28	0.25	0.11	0.17	0.19
AVE = 0.84									
3.PerMor	PerMor1	0.20	0.36	**0.80**	0.32	0.42	0.21	0.33	0.34
CR = 0.83	PerMor2	0.05	0.16	**0.86**	0.17	0.32	0.12	0.31	0.29
AVE = 0.62	PerMor3	0.19	0.17	**0.69**	0.21	0.31	0.15	0.29	0.28
4. ProJus	ProJus1	0.30	0.31	0.28	**0.92**	0.38	0.44	0.45	0.36
CR = 0.94	ProJus2	0.27	0.26	0.27	**0.95**	0.39	0.54	0.51	0.35
AVE = 0.84	ProJus3	0.27	0.20	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	0.15	0.21	0.43	0.42	**0.92**	0.27	0.45	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	**0.97**	0.58	0.23
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	0.38	0.45	0.22	0.36	**0.95**
AVE=0.82	Intent3	0.24	0.18	0.38	0.41	0.46	0.26	0.42	**0.93**

SanPro – sanction certainty; SanSev – sanction severity; PerMor – personal Moral Beliefs; ProJus – procedure justice; DisJus – distributive justice; IntJus – Interpersonal Justice; InfJus – informational justice; Intent – intention to comply with Internet use policy.

Table 3. Discriminant validity of measurement model

	1	2	3	4	5	6	7	8
1. SanPro	**0.92**							
2. SanSev	0.54**	**0.92**						
3. PerMor	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**

Note: Diagonal elements are the square root of the AVE values. Off-diagonal elements are the correlations among latent constructs, **p < 0.01.

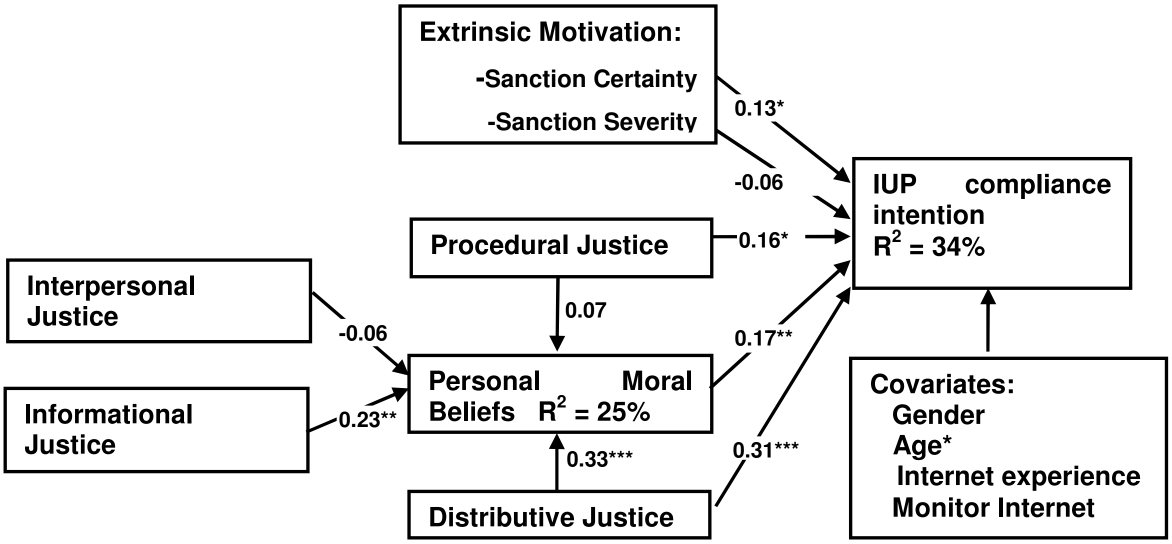

Figure 2. Results of testing hypotheses using PLS analysis. Completely standardized estimates, controlled for covariates in the research model, *p < 0.05, **p < 0.01, ***p<0.001.

Discussion

Key Findings and Limitations

We employed an integrated 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 organizational justice and intrinsic personal moral beliefs against Internet abuses. Sanction mechanisms, although less effective than personal moral beliefs (as shown later), also shape IUP compliance intention. The deterrence effect of formal sanction is largely exerted through sanction certainty rather than sanction severity. The non-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 relative 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, as one primary characteristic of organizations, not only influences IUP compliance intention directly but also indirectly through fostering favorable personal moral beliefs against Internet abuses. In particular, distributive justice was found to promote IUP compliance intention both directly and indirectly through personal moral beliefs. Procedural justice was found to only exert direct influence on IUP compliance intention. Information justice indirectly influences IUP compliance intention through personal moral beliefs.

The hypothesized indirect effects of procedural justice and interpersonal justice through personal moral beliefs were not supported in this study. The effect of procedural justice on personal moral beliefs 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 moral beliefs than procedural justice. The insignificance 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 et al. 2000).

We also conducted a post-hoc analysis to test whether interpersonal and information justice directly impact IUP compliance intention. An alternative model was built by including two direct links between those two justice dimensions and compliance intention. These two direct links were found to be insignificant. The significance level of other variables stays the same. Therefore, the effect of information justice is fully mediated through personal moral beliefs. Interpersonal justice has neither a direct nor an indirect impact on IUP compliance intention.

We further compared the relative efficacy of our research model with the one that only considered formal sanctions in explaining IUP compliance intention. An alternative model was built by incorporating perceived sanction certainty, sanction severity and the control variables to predict IUP compliance intention. The R^2 of the alternative model is only 10.0% in comparison to 34% of our research model. The result suggests that personal moral beliefs and organizational justice are two dominant factors in explaining IUP compliance intention.

Our study also has some limitations. One limitation is the use of behavioral 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 (TRA) (Fishbein et al. 1975). According to TRA, behavioral intention is a strong predictor of actual behavior. But future studies could be conducted to test our research model by actually monitoring employees' actual compliance behavior. Another limitation is that our study 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 extensible to severe cyber crimes.

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 high moral beliefs 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 et al. 2009a; Herath et al. 2009b; Li et al. 2010a). 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 moral beliefs. A high level of informational justice and distributive justice could help organizations enhance an employee's moral beliefs against Internet abuses. This finding suggests that one's moral belief 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. Beside organizational justice, an employee's moral beliefs against 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 cyber crimes may increase an employee's moral beliefs against Internet abuses.

Implications for Practice

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 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.

Since 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 their intrinsic motivation to comply with the IUP. This may cause employees accept IUP voluntarily even when they are unlikely to be caught and punished for Internet abuses. Organizations should focus on organizational justice and emphasizing personal values, i.e. personal moral beliefs against Internet abuses.

Further, the findings suggest that distributive and informational justice is effective in shaping individual employees' personal moral beliefs against Internet abuses. Organizations need to explicitly educate their employees about benefits from restricting personal Internet activities at the workplace by emphasizing the negative impact of Internet abuses. For example, Bock and Ho (2009) empirically found the negative impact of non-work-related emails and personal Internet usage on 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 also need to ensure informational justice when implementing IUP. Informational justice could be engendered through periodical information security training or security awareness campaigns to communicate with employees about the IUP.

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 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 moral values of employees and perceived organizational justice in dealing with IUP violations.

References

Bagozzi, R.P., and Yi, Y. "On the evaluation of structural equation models," *Journal of the Academy of Marketing Science* (16:1) 1988, pp 74-94.

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

Bock, G.-W., and Ho, S.L. "Non-work related computing (NWRC)," *Communications of the ACM* (52:4) 2009, pp 124-128.

Chin, W.W., Marcolin, B.L., and Newsted, P.R. "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* (14:2) 2003, pp 189-217.

Cohen-Charash, Y., and Spector, P.E. "The role of justice in organizations: A meta-analysis," *Organizational Behavior and Human Decision Processes* (86:2) 2001, pp 278-321.

Colquitt, J.A. "On the dimensionality of organizational justice: A construct validation of a measure," *Journal of Applied Psychology* (86:3) 2001, pp 386-400.

D'Arcy, J., Hovav, A., and Galletta, D. "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research* (20:1) 2009, pp 79-98.

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

Fornell, C., and Larcker, D. "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research* (18:1) 1981, pp 39-50.

Gefen, D., and Straub, D. "A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example," *Communications of the AIS* (16:5) 2005, pp 91-109.

Greenberg, J. "The social side of fairness: Interpersonal and informational classes of organizational justice," in: *Justice in the workplace: Approaching fairness in human resource management* R. Cropanzano (ed.), Erlbaum, Hillsdale, NJ, 1993, pp. 79-103.

Herath, T., and Rao, H.R. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems* (47:.2) 2009a.

Herath, T., and Rao, H.R. "Protection motivation and deterrence: a framework for security policy compliance in organizations," *European Journal of Information Systems* (18:2) 2009b, pp 106-125.

Hoffman, K.D., and Kelley, S.W. "Perceived justice needs and recovery evaluation: A contingency approach," *European Journal of Marketing* (34:3-4) 2000, pp 418-432.

Kim, W.C., and Mauborgne, R.A. "Procedural justice, attitudes, and subsidiary top management compliance with multinationals' corporate strategic decisions," *Academy of Management Journal* (36:3) 1993, pp 502-526.

Lau, V.C.S., Au, W.T., and Ho, J.M.C. "A qualitative and quantitative review of antecedents of counterproductive behavior in organizations," *Journal of Business and Psychology* (18:1) 2003, pp 73-99.

Li, H., Sarathy, R., and Xu, H. "Understanding situational online information disclosure as a privacy calculus," *Journal of Computer Information Systems* (Forthcoming) 2010a.

Li, H., Zhang, J., and Sarathy, R. "Understanding compliance with internet use policy from the perspective of rational choice theory " *Decision Support Systems* (48:4) 2010b, pp 635-645.

Lim, V.K.G. "The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice," *Journal of Organizational Behavior* (23:5) 2002, pp 675-694.

Limayem, M., Khalifa, M., and Chin, W.W. "Factors motivating software piracy: a longitudinal study," Proceedings of the International Conference on Information Systems, North Carolina, United States, 1999, pp. 124-131.

Lindell, M.K., and Whitney, D.J. "Accounting for common method variance in cross-sectional research designs," *Journal of Applied Psychology* (86:1) 2001, pp 114-121.

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

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

Paternoster, R., and Simpson, S. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law & Society Review* (30:3) 1996, pp 549-583.

Peace, A.G., Galletta, D., and Thong, J. "Software piracy in the workplace: A model and empirical test," *Journal of Management Information Systems* (20:1) 2003, pp 153-177.

Pee, L.G., Woon, I.M.Y., and Kankanhalli, A. "Explaining non-work-related computing in the workplace: A comparison of alternative models," *Information & Management* (45:2) 2008, pp 120-130.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y., and Podsakoff., N.P. "Common method biases in behavior research: A critical review of the literature and recommended remedies," *Journal of Applied Psychology* (88:5) 2003, pp 879-903.

Sindhav, B., Holland, J., Rodie, A.R., Adidam, P.T., and Pol, L.G. "The impact of perceived fairness on satisfaction: Are airport security measures fair? Does it matter?," *Journal of Marketing Theory and Practice* (14:4) 2006, pp 323-335.

Siponen, M., Pahnila, S., and Mahmood, A. "Factors influencing protection motivation and IS security policy compliance," in: *Innovations in Information Technology 2006*, Dubai, 2006, pp. 1-5.

Sophos "Sophos security threat report," 2009.

Straub, D.W. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3) 1990, pp 255-276.

Turel, O., Yuan, Y., and Connelly, C.E. "In justice we trust: Predicting user acceptance of e-commerce service," *Journal of Management Information Systems* (24:4) 2008, pp 123-151.

Tyler, T.R. "The psychology of legitimacy: A relational perspective on voluntary deference to authorities," *Personality and Social Psychology Review* (1:4) 1997, pp 323-345.

Tyler, T.R. "Restorative justice and procedural justice: Dealing with rule breaking," *Journal of Social Issues* (62:2) 2006, pp 307-326.

Tyler, T.R., Callahan, P.E., and Frost, J. "Armed, and dangerous (?): Motivating rule adherence among agents of social control," *Law & Society Review* (41:2) 2007, pp 457-492.

Wenzel, M. "The social side of sanctions: Personal and Social Norms as Moderators of Deterrence," *Law and Human Behavior* (28:5) 2004, pp 547-567.

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

Young, K.S., and Case, C.J. "Internet abuse in the workplace: New trends in risk management," *Cyberpsychology & Behavior* (7:1) 2004, pp 105-111.