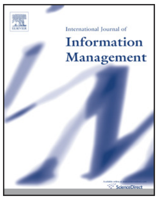
International Journal of Information Management 36 (2016) 309–321

Contents lists available at ScienceDirect

International Journal of Information Management

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



Procedural justice to enhance compliance with non-work-related computing (NWRC) rules: Its determinants and interaction with privacy concerns

Jai-Yeol Son*, Jongpil Park

School of Business, Yonsei University, 50 Yonsei-ro, Seoul 120-749, South Korea

ARTICLE INFO

Article history:
Received 4 February 2015
Received in revised form 3 December 2015
Accepted 10 December 2015
Available online 4 January 2016

Keywords:
Non-work-related computing
Organisational justice
Procedural justice
Privacy concerns
Compliance behaviour

ABSTRACT

Computing resources are essential to foster the productivity of employees in organisations; however, non-work-related computing (NWRC) in the workplace has recently become a serious concern because employees often spend too much time in the personal use of computers. To deepen our understanding of employees' compliance with NWRC rules, we developed and tested a research model that focuses on the formation of procedural justice and moderating role of privacy concerns. The results indicate that employees are more willing to comply with NWRC rules when they believe fair procedures to be in place during the design and implementation of the rules. In addition, accuracy, consistency, and ethicality were found to enhance employees' belief in procedural justice. Further, we found that the effect of procedural justice on compliance intention is moderated by privacy concerns that arise from the implementation of NWRC rules.

1. Introduction

Non-work-related computing (NWRC), defined as employees' use of computers at work for nonwork or personal purposes (Bock & Ho, 2009), has become a serious issue. From 60% to 80% of employees' time on the Web at work is wasted with nonwork activities (Strozniak, 2013). Workers in the U.S. surf the Web for nonwork purposes for one to two hours a day, which costs organisations billions of dollars in lost productivity (Blanding, 2011). An internal investigation by J.C. Penny Co., found that 4800 employees at its headquarter watched about 5 million YouTube videos in one month (Madrigal, 2013).

Of course, it is often argued that NWRC could favourably affect employee productivity by fostering creativity, learning, and well-being. However, organisations should not underestimate either productivity lost to NWRC or potential risks from employees' misconduct while engaging in NWRC. The average American worker spends more than two hours each day for the personal use of the Internet, which can be estimated as about US$85 billion annually in lost productivity for U.S. companies (Palmquist, 2013). Employers in the UK lose about €300 million annually in lost productivity due to their employees' gambling online at work (Taylor, 2007). Productivity loss caused by NWRC is problematic, especially when employees with addictive tendencies become addicted to use of the Internet (Stanton, 2002). Just as people often become addicted to alcohol, an increasing number of users are expected to become addicted to the Internet (Young & Rogers, 1998).

Because of these concerns, an increasing number of organisations have introduced policies to monitor and curtail their employees' engagement in NWRC. However, resistance from employees becomes the biggest issue when organisations implement NWRC rules and monitor their employees' activity on computers accordingly. This monitoring and associated punishment for noncompliance with NWRC rules may offend employees by causing them to feel undervalued and distrusted. Consequently, their job satisfaction and work morale may suffer. Employees are often found to retaliate against enhanced information security policies by engaging in reactive computer abuse behaviours (Lowry, Posey, Bennett, & Roberts, 2015). This potential for disruptions makes it critical for organisations to carefully introduce NWRC rules so as to minimize resistance from employees.

Much research on employees' compliance with policies on IS misuse applied general deterrence theory (GDT) as its theoretical lens (Siponen & Vance, 2010). However, the findings from the research based on GDT-based factors such as certainty of sanctions and severity of sanctions were mixed (Lowry et al., 2015; Willison & Warkentin, 2013). It appears that the deterrence-based approach in organisations does not work very well in increasing employ-

* Corresponding author. Fax: +82 2 2123 8639.
E-mail addresses: json@yonsei.ac.kr (J.-Y. Son), davidpark@yonsei.ac.kr (J. Park).

http://dx.doi.org/10.1016/j.ijinfomgt.2015.12.005
0268-4012/© 2015 Elsevier Ltd. All rights reserved.

ees' passive compliance with IS misuse polices. This also leads the research stream to move from passive compliance to proactive compliance. As such, IS researchers have attempted to apply theoretical lenses, such as intrinsic motivation model (Son, 2009), protection motivation theory (Herath & Rao, 2009a), and rational choice theory (Bulgurcu, Cavusoglu, & Benbasat, 2010).

In a similar vein, Willison and Warkentin, (2013) have recently identified organisational justice as an underresearched area in understanding employees' compliance with security policies in the workplace. Several studies have already applied the justice framework (e.g., Lim, 2002; Posey, Bennett, Roberts, & Lowry, 2011; Henle, Kohut, & Booth, 2009; De Lara, 2007). This paper is in line with these studies based on the justice framework. Of course, the justice framework was also heavily applied in prior research that examined employees' compliance with organisational policies other than those on IS misuse. However, unlike other organisational policies (e.g. policies on drug, alcohol, violence, etc.) that are accepted by employees with less resistance, employees often do not consider noncompliance of polices on IS misuse including NWRC rules as a serious issue and thus waste much time at work online. Worse, they often abuse computing assets of their organisations as a retaliatory response to enhanced polices on IS misuse (Lowry et al., 2015). In this sense, it seems necessary to examine if the justice framework can also be well applied within the context of employees' compliance with NWRC rules.

This paper intends to contribute to the literature by offering a comprehensive understanding on the formation of procedural justice when their employers deploy NWRC rules. Based on the review of the literature, five potential antecedents – accuracy, consistency, correctability, participation, and ethicality – of procedural justice are identified to gain greater insight into how employees develop their belief in procedural justice when their employers introduce NWRC rules. Further, our study examines the moderating role of privacy concerns on the relationship between procedural justice and employees' intention to comply with NWRC rules.

2. Literature review

Compliance in this study refers to employees' acquiescence to their employer's request to comply with NWRC rules. Recently, IS scholars have paid greater attention to employees' compliance behaviours as an important subject. This is largely because scholars have focused more on the socio-organisational and human issues of the management of information security (Dhillon & Backhouse, 2000). To this end, most of the scholarly effort to understand employees' compliance behaviours in IS has been undertaken within the context of security management (Kwon & Johnson 2013). Scholars in this area have often developed theory-based research models, and used data collected by administering questionnaire surveys to test employees' motivation to comply with organisational policies on IS security.

A review of theory-based empirical studies on compliance behaviour in IS reveals that much work used GDT to offer a theoretical explanation (see Table 1 for the summary). GDT, originally developed by Ehrlich, (1973), has been widely applied to understand how to deter individuals from participating in illegal and deviant behaviours. GDT suggests that people are less likely to engage in illegal or deviant behaviours when they perceive that such behaviours can result in sanctions, punishment, or other disincentives. Specifically, GDT posits two central tenets – certainty of sanctions and severity of sanctions – that can deter individuals from illegal or deviant behaviours (Peace, Galletta, & Thong, 2003). However, studies with GDT-based factors offered mixed results on the efficacy of GDT as a theoretical base in understanding employees' compliance with IS misuse policies (Lowry et al., 2015; Willison & Warkentin, 2013).

For instance, some studies reported that GDT-based factors do not have a significant relationship with employees' compliance intention (D'Arcy, Hovav, & Galletta, 2009; Hu, Xu, Dinev, & Ling, 2011; Son, 2011). D'Arcy et al. (2009) reported that, while perceived severity of sanctions has a strong negative association with employees' misuse of IS assets in organisations, perceived certainty of sanctions does not have a strong relationship. Hu et al. (2011) developed and tested a research model based on GDT and rational choice calculus. However, they did not find a strong impact of perceived deterrence – in terms of certainty, severity, and celerity of sanctions – on employees' intention to commit computer misconduct. Other research with GDT-based factors often reported findings that appear contrary to the theoretical reasoning (Herath & Rao, 2009a, 2009b). For instance, Herath and Rao (2009a) found that, while certainty of detection has a positive effect on employees' intention to comply with a security policy, severity of punishment has a negative effect.

Given that the efficacy of GDT was questioned in the prior research, scholarly effort was made to offer alternative theoretical explanations on user compliance with IS misuse policies. Lowry et al. (2015) applied fairness and psychological reactance theories and found that employees often engage in reactive computer abuse as an undesirable response to organisational effort to protect information assets from employee security threat. Li, Zhang, and Sarathy (2010) applied rational choice theory and found that, while perceived benefits from Internet abuse has a negative effect on Internet use policy compliance intention, perceived risks, such as detection probability and security risks, have positive effects on the intention. Bulgurcu et al. (2010) also applied rational choice theory and found that employees' intention to comply with IS security policies were significantly influenced by attitudes toward compliance with the policies. Specifically, the attitudes were found to be shaped by employees' beliefs about the overall consequences of compliance or noncompliance. Several variables such as intrinsic benefit, safety, and work impediments were also found to predict the overall consequences of compliance or noncompliance.

Scholars have paid special attention to the justice framework as a useful theoretical lens in understanding employees' compliance with IS misuse policies. For instance, Lim (2002) found that when employees perceive their employers to be fair in terms of distributive, procedural, and interactional standards, they were less likely to employ a neutralization technique through metaphor of the ledger. In addition, she found that employees are less likely to engage in cyberloafing when they cannot legitimize the act through the metaphor of the ledger. Henle et al. (2009) found that zero tolerance and progressive discipline during the disciplinary procedures increase the perception of policy fairness related to cyberloafing. In addition, formal appeal processes have a positive impact on the perception of policy fairness related to cyberloafing.

Our study intends to extend the research stream on the application of the justice framework to the understanding of user compliance with IS misuse policies. To do so, of the several types of organisational justice (e.g., procedural, distributive, and informational), we pay particular attention to the role of procedural justice because the current study aims to understand how organisations can provide fair procedures during the implementation of NWRC rules.[1] Despite the scholarly effort on the application of jus-

[1] Of course, we do not exclude the potential importance of the other types of organisational justice (e.g., distributive and interactional) in explaining employees' compliance with NWRC rules. However, examination of all the antecedents of all three types of organisational justice could well be beyond the scope of a single study.