Journal of Organizational and End User Computing
Volume 31 • Issue 1 • January-March 2019

Protective Measures and Security Policy Non-Compliance Intention:
IT Vision Conflict as a Moderator

Kuo-Chung Chang, Yuan Ze University, Taoyuan, Taiwan
Yoke May Seow, Yuan Ze University, Taoyuan, Taiwan

ABSTRACT

Internal vulnerabilities and insider threats top the list of information security (InfoSec) incidents; prompting organizations to establish InfoSec policy (ISP). Yet, mitigating user's ISP non-compliance is still an arduous task. Hence, this study aims to minimize user's ISP non-compliance intention by investigating their perception and attitude toward ISP non-compliance. Specifically, protective measures drawing upon the protection motivation theory - perceived severity of ISP non-compliance, rewards and familiarity with ISP - analyze users' attitude toward ISP non-compliance. Further, the new construct, information technology (IT) vision conflict, is the mismatch between the values that users hold and those embedded in the ISP. The misalignment of the two conflicting values moderates the relationship between the protective measures and attitude toward ISP non-compliance. Findings show that IT vision conflict weakens the negative relationship between perceived severity of ISP non-compliance and attitude toward ISP non-compliance; indirectly affecting ISP non-compliance intention.

KEYWORDS

Familiarity With Information Security Policy, Information Security Policy Non-Compliance Intention, Information Security, IT Vision Conflict, Perceived Severity, Protection Motivation Theory, Rewards

INTRODUCTION

In 2015, organizations in the United Kingdom (UK) reported a 36% increase of employee-related information security (InfoSec) breaches compared with the previous year (PwC, 2015b); and insider threats constitute the highest number of InfoSec incidents globally (PwC, 2015a). Nonetheless, although organizations have implemented InfoSec policy (ISP) (Guo, Yuan, Archer, & Connelly, 2011), users' resistance to ISP is among the major reasons for ISP's failure (Kolkowska & Dhillon, 2013) which is a notable problem for organizations (Posey, Roberts, Lowry, Bennett, & Courtney, 2013). Employees disregarded the ISP because they felt that the ISP is a nuisance (Renaud, 2012), they prioritize other work tasks, and the ISP is poorly understood (PwC, 2015b). Also, ISP non-

DOI: 10.4018/JOEUC.2019010101

compliance behaviors could be due to employees' dissatisfaction with the ISP (Hedström, Karlsson, & Kolkowska, 2013), negligence or ignorance (Siponen & Vance, 2010).

Thus, the domains of InfoSec and ISP non-compliance have received substantial attention from researchers and practitioners. Among the behavioral theories applied to address ISP non-compliance include deterrence theory (D'Arcy & Hovav, 2009; Herath & Rao, 2009), the theory of planned behavior (Bulgurcu, Cavusoglu, & Benbasat, 2010; Cox, 2012), and social action theory (Hedström et al., 2013). Further, there are research investigating user ISP non-compliance behaviors from ethical (Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009) and rational choice perspectives (Bulgurcu et al., 2010; Vance & Siponen, 2012).

While extant research offers insights on the InfoSec contravention, they leave an incomplete understanding of the ISP infringement issues. First, despite having identified factors of ISP compliance behaviors, research highlighting ISP non-compliance behaviors is scant (Guo et al., 2011; Workman, Bommer, & Straub, 2008). Moreover, these two types of behaviors are qualitatively dissimilar and therefore, their respective antecedents might differ (Guo et al., 2011). Adhering rules or policy could simply be based on normative beliefs regulating what people ought to do without requiring the users to over analyze (Cox, 2012). However, to perform counter-normative actions, users might deliberate about rule-breaking and find relevant excuses (Blanton & Christie, 2003). Furthermore, Wall et al. (2013) claim that habitual behavior, being routine and automatic, is imperative in mitigating ISP non-compliance. In contrast, users might think twice before committing the ISP non-compliance action because they know that it is unlawful. Hence, it is more worthwhile to investigate why users are ISP non-compliant rather than why they are ISP-compliant (Guo et al., 2011; Vance & Siponen, 2012). This is even more so since intentional negligence of ISP is one of the most common security-related behaviors among users. Investigating the ISP non-compliance phenomenon is more pragmatic and interesting because unexpected deviant actions have greater "informational value" than normative behaviors (Barlow, Warkentin, Ormond, & Dennis, 2013; Blanton & Christie, 2003); while extending our understanding on ISP non-compliance motivation or rationalization (Siponen & Vance, 2010).

Secondly, employees might pose significant InfoSec risks for their intentional negligence and ignorance of the ISP (Posey et al., 2013). Nonetheless, extant studies generally focus on deterrent and preventive strategies (e.g., sanctions, awareness programs, incentives and disincentives) to mitigate ISP contravention (Herath & Rao, 2009; Herath & Rao, 2009; Vance & Siponen, 2012). Moreover, ISP violation behaviors, conceptualized as a generic term, encompass both malicious and non-malicious behaviors. Malicious behavior involves illegal and unethical security violations such as hacking, coding viruses, stealing and/or selling confidential information (Guo et al., 2011; Posey, Roberts, Lowry & Hightower, 2014). For these malicious actions, offenders intend to obtain personal gains at the expense of the focal organization (Cox, 2012; Guo et al., 2011). In contrast, non-malicious behavior entails omissive (Workman et al., 2008) and other ignorant and negligent actions with non-spiteful intent (e.g., failed to update passwords and security patches; and stored sensitive data in unencrypted storage devices). Those offenders engage in non-malicious ISP violation not for personal gains, such as improving efficiency and assisting others (Kolkowska & Dhillon, 2013; Renaud & Goucher, 2012; Vance & Siponen, 2012). Therefore, by examining both malicious and non-malicious behaviors concurrently, the effects of the antecedents on ISP violations are elusive (D'Arcy & Hovav, 2009; Siponen & Vance, 2010).

This present study particularly focuses on ISP non-malicious violation intention by exploring the potential factors that mitigate user's ISP non-compliance intention. ISP is conceived as a nuisance to employees and perceived as a kind of threat to their convenience and productivity (Kolkowska & Dhillon, 2013; Lowry & Moody, 2013). Therefore, employees take non-compliance behaviors as a coping strategy to protect their interests and regain what has been lost due to ISP implementation (Hedström et al., 2013). Thus, the authors believe that the protection motivation theory (PMT) (Rogers, 1975) is appropriate to investigate potential factors that mitigate ISP non-compliance intention. PMT posits that a perceived threat would prompt the individual to cognitively appraise the threats and