Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Understanding information security stress: Focusing on the type of information security compliance activity

Chunghun Lee [a], Choong C. Lee [a,*], Suhyun Kim [b]

[a] Graduate School of Information, Yonsei University, 262 Seongsanno, Seodaemun-gu, Seoul, Republic of Korea
[b] IT Outsourcing, GS ITM, 31 Gyedong-ro, Jongro-gu, Seoul, Republic of Korea

ARTICLE INFO

Article history:
Received 23 July 2015
Received in revised form 4 January 2016
Accepted 4 February 2016
Available online 18 February 2016

Keywords:
Information security stress
Information security policy
Information security compliance
Person and environment fit model
Work overload
Invasion of privacy

ABSTRACT

Organizations are intensifying their information security levels, as information security has become an essential element in business management. However, excessive focus on the mere reinforcement of information security has placed employees under stress. Studies have confirmed that the negative effects of stress include reduced employee productivity. Therefore, it is important to manage employee stress while enforcing information security in an organization. Based on person–environment fit theory, this study examines how employees become stressed, the factors behind information security stress (ISS), and the differences between managerial and technical security-oriented organizations. The results show that work overload and invasion of privacy are information security stressors. Furthermore, work overload has a greater effect on ISS in managerial security-oriented organizations, while invasion of privacy exerts a greater influence on ISS in technical security-oriented organizations. In addition, attitude to compliance with the information security policy mitigates work overload and invasion of privacy. These findings can be used as a basic reference for the establishment of employee stress management measures and the evaluation of information security stress levels.

1. Introduction

Organizational efforts to protect information assets are increasingly mandated by government regulations and standards due to the increasing threats and cost of security failure. These efforts consist mainly of the introduction of new technical and managerial preventive schemes and the enforcement of employee compliance with tighter information security policies and technical obligations. This process has imposed a heavy burden on all organizational members that can no longer be ignored. A survey conducted by Macromill Embrain (2014), a marketing research firm, shows that 63.6% of respondents have experienced stressful incidents because of information security compliance activities (ISCAs) and that 42.7% have had problems carrying out their work because of them. The stress from security requirements has negative effects on ISCAs. It makes employees show stressful reaction to information security policy (ISP) (Puhakainen and Siponen, 2010) and indirectly reduces their compliance intention (Bulgurcu et al., 2010). As a result of enhanced security requirements, information security stress (ISS) results in employees' ISP violation (D'Arcy et al., 2014). Considering the direct negative effect of this new stress on employee' productivity, the rising stress level due to ISCAs requires urgent attention. The research has already verified that stress reduces employees' morale and job satisfaction,

* *Corresponding author.* Tel.: +82 2 2123 4186.
E-mail addresses: goguming@gmail.com (C. Lee), cclee@yonsei.ac.kr (C.C. Lee), canopus420@gmail.com (S. Kim).
http://dx.doi.org/10.1016/j.cose.2016.02.004
0167-4048/

negatively impacting organizations (Jackson and Schuler, 1985; Jex and Beehr, 1991; Ragu-Nathan et al., 2008). Thus, it is important for organizations to understand the severity of information security stress (ISS) and its causes.

The research has empirically examined the job stress experienced by information security officers (Burke and Cooper, 2000; Cooper et al., 2001; Kinman and Jones, 2005; Moore, 2000; O'Driscoll and Beehr, 1994) and the technostress felt by employees using new information technology (Ayyagari et al., 2011; Tu et al., 2005). D'Arcy et al. (2014) examined that security-related stress is the main cause of employees' ISP violation. However, there are still very few empirical studies on ISS and its antecedents from the IS user side.

This study investigates the degree to which two major stressors – work overload and invasion of privacy in the context of job stress and technostress – can be applied to ISS and identifies the factors mitigating these two stressors. The person–environment fit (P–E fit) theory is used as a theoretical basis from which to hypothesize the valuables that ease the stressors. There is a big difference between managerial and technical security (von Solms, 1998). Managerial security focuses on improving employees' security awareness and behavioral security measures, while technical security centers on applying security applications. Given the clear difference between the ISCAs' managerial and technical compliance activities, we also examine the differences in the research model's loading magnitude and causality between two groups of organizations in which one activity or the other is emphasized.

The rest of this paper is organized as follows. First, the ISCA, stress sources, other research variables considered in the research model, and studies relevant to P–E fit theory are reviewed. The research model and hypotheses are then introduced, and the research methods are explained. Finally, the study's theoretical and practical implications are discussed after the research findings are outlined.

2. Conceptual background

2.1. *The importance of factors related to individuals in information security compliance activities (ISCAs)*

Information security compliance activities are a series of activities that comply with managerial and technical information security policies (ISPs), which are written statements on the roles and responsibilities employees must fulfill in order to protect important information in their organizations (Boss and Kirsch, 2007; Dhillon and Backhouse, 2001; Herath and Rao, 2009). The ISP strengthens firms' security levels by preventing employees' exploitation of information assets and information security accidents (Wen, 1998). The ISP is made for employees to use as a security guideline for the use of information systems in their work (Whitman et al., 2001).

As organizational information security used to center on the application and enforcement of security technologies, much of the research also focused on the development and use of security technologies (Fernandez-Medina et al., 2006; Vroblefski et al., 2005). However, the research focus is shifting toward managerial security for internal employees authorized for system use or facility access, as ignorance, mistakes, and deliberate acts can cause security failures (Durgin, 2007; Lee and Lee, 2002; Lee et al., 2003). Furthermore, an insider is the major source of data breaches (Chen et al., 2012; Ponemon Institute, 2015). According to the Symantec report, 47% of data breaches occurred by insiders in 2010 (Wall, 2011), and companies have invested significant resources to address insider threats (PricewaterhouseCoopers, 2013). Therefore, it is important that organizations invest in both managerial and technological security in order to maximize their effects (Bulgurcu et al., 2010; Pahnila et al., 2007). As ISCAs shift from a technical perspective to an individual and organizational one, the managerial security applied to ensure employee compliance with ISPs has become the key issue for organizational information security.

Recent studies on information security at an individual level seek to identify the factors that encourage employees to comply with the ISP (Furnell and Clarke, 2012; Safa et al., 2015). An effective consideration of these factors can help organizations make employees actively participate in ISCAs and reduce their negative effects, such as work overload and invasion of privacy.

2.2. *The stressors of ISS: work overload and invasion of privacy*

Stress can be classified as a 1) stimuli-based concept in which stress is an independent variable, a 2) response-based concept in which stress is a dependent variable, or a 3) transaction-based concept in which stress is a process (Jex, 1998). This study considers ISS from the transaction-based perspective, which posits that stress is the result of an interaction between external environmental stimuli and an individual's reactions to them. Information security stress occurs during the process in which employees attempt to comply with information security policy (ISP).

Stress arises when the environmental demands exceed individual's abilities (Cooper et al., 2001; Lazarus, 1995). This overall transaction process constitutes the experience of stress (Ayyagari et al., 2011). Stressors manifest as the stressful stimuli encountered by individuals, and stress is the individual's psychological response to the stressors (Cooper et al., 2001).

The stressors that cause ISS can be deduced from technostressors and job stressors, which have been discussed by a number of studies on employee stress (Ayyagari et al., 2011; Burke and Cooper, 2000; Cooper et al., 2001; Kinman and Jones, 2005; Moore, 2000; O'Driscoll and Beehr, 1994; Tu et al., 2005). An ISP is an employee obligation and is thus similar to a duty. Information security technology affects employees and business processes as routinely as ICT (information and communication technology) does.

Following Ayyagari et al. (2011) and Moore (2000), widely used in studies on job stress and technostress, we identified two major stressors: work overload and invasion of privacy.

First, ISP imposes a new administrative burden on employees' daily work. Its series of cumbersome restraints and inconveniences create extra work and affect employee productivity (D'Arcy et al., 2014).

Second, an important part of ISP assumes tight monitoring over employees' information security compliance activities. Surveillance control techniques are becoming more common in social spaces, including workplaces. Employees can be intimidated and see this as a violation of privacy, as the