Computers in Human Behavior 81 (2018) 282–293

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Examining technostress creators and role stress as potential threats to employees' information security compliance

Inho Hwang [a], Oona Cha [b, *]

[a] The Center for Continuing Education, Kyung Hee University, 26, Kyungheedae-ro, Dongdaemun-gu, Seoul, 02447, Republic of Korea
[b] School of Business Administration, Chung-Ang University, 84, Heukseok-ro, Dongjak-gu, Seoul, 06974, Republic of Korea

ARTICLE INFO

Article history:

Keywords:
Information security
Technostress
Role stress
Regulatory focus
Organizational commitment
Compliance intention

ABSTRACT

This study examined whether employees' security-related stress, i.e., technostress and role stress, in an organizational setting could affect their compliance intention regarding information security. In a survey of 346 employees, it was found that security-related technostress creators in organizations negatively affected employees' organizational commitment, both directly and indirectly through role stress, and further lowered compliance intention regarding information security. In addition, it was found that employees' regulatory focus, i.e., promotion focus, moderated the relationship between technostress creators and role stress. Employees with a high level of promotion focus were more resistant to the adverse effect of technostress creators and thus experienced less role stress. These results suggest directions for organizational strategies to manage and enhance employees' information security compliance.

1. Introduction

Organizations are increasing investment in information security technology to battle various security threats. The worldwide revenues for security-related hardware, software, and services are expected to grow from $73.7 billion US dollars in 2016 to $101.6 billion US dollars by 2020 (IDC, 2016). In addition, information security systems are adopting more complex and specialized technology to respond to the diversified threats to information security (Guo, 2013; Hwang, Kim, Kim, & Kim, 2017). These technologies include device control technology (e.g., personal PC, USB, and other personal devices), network firewall technology (e.g., detecting critical information leaks via web mail, messenger, web hardware), network monitoring technology (e.g., based on protocols such as HTTP, FTP, and SMTP), document security technology (e.g., encryption technology for important documents, control technology for document access) and security management technology (e.g., management of passwords, vaccines and O/S programs), to name a few.

Being equipped with up-to-date and advanced information security technology and systems is helpful for fighting various security threats, and it is not surprising that it has become the utmost concern for most organizations. However, there is something largely ignored in the picture: people who are affected by the system and who have to deal with the technology on a daily basis. If not properly managed, employees may struggle to adapt to complex and unfamiliar technology of the security system and to deal with additional workload and uncertain procedures imposed by the security protocol, which can lead to an increased level of stress on the job (D'Arcy, Herath, & Shoss, 2014). This stress due to technology use (or "technostress") can induce various negative organizational outcomes. For example, Tarafdar, Tu, Ragu-Nathan, and Ragu-Nathan (2007) have suggested that conditions that create technostress are associated with adverse psychological outcomes such as an increased level of role stress, reduced job satisfaction and reduced organizational commitment, as well as with adverse information system (IS) outcomes such as decreased innovation in employees' tasks while using the IS, reduced productivity when using the IS and dissatisfaction with the IS. This line of thought poses a question: is it possible that employees' stress due to technological aspects of information security itself negatively affects their compliance toward information security?

2. Theoretical background and hypotheses

Previous literature on information security has presented

* Corresponding author.
E-mail addresses: hwanginho@nate.com (I. Hwang), ocha@cau.ac.kr (O. Cha).

https://doi.org/10.1016/j.chb.2017.12.022
0747-5632/© 2017 Elsevier Ltd. All rights reserved.

various directions for predicting employees' information security compliance, largely focusing on employees' attitude, motivation and rational choice. Some studies focused on employees' attitude toward information security and used the framework of the theory of planned behavior (Ajzen, 1991) to predict employees' compliance intention and behavior (e.g., Safa & Von Solms, 2016). Other studies focused on employees' motivation: some focused on factors enhancing extrinsic motivation (e.g., sanction or social pressure) and/or intrinsic motivation (e.g., value congruence) to predict employees' compliance intention (Herath & Rao, 2009; Son, 2011). Still, some focused on how employees deal with security threats based on protection motivation theory (Maddux & Rogers, 1983; Rogers, 1975, 1983; Witte, 1996) and examined how factors regarding threat appraisals (e.g., vulnerability or severity of threat) and coping appraisals (e.g., self-efficacy or response efficacy) affected employees' reaction to security threats (Boss, Galletta, Lowry, Moody, & Polak, 2015; Chen & Zahedi, 2016; Ifinedo, 2012; Safa et al., 2015; Vance, Siponen, & Pahnila, 2012). Finally, research based on rational choice theory claims that employees' compliance reflects their analysis of the benefits and costs of security compliance (Bulgurcu et al., 2010; Hu, Xu, Dinev, & Ling, 2011) (see Sommestad, Hallberg, Lundholm, and Bengtsson (2014) for a review).

However, literature on information security seems to lack concern for the technological aspects of information security itself and their adverse impact on employees. Aside from organizational efforts to reward or punish security-related behavior or employees' individual attitudes or motivation to comply with information security policies in an organization, employees at all levels have to face and deal with complexity, overload, and uncertainty of information technology in their jobs every day. In addition, employees might have to deal with various situations where the organization's information security compliance goal interferes with their goal on the job to achieve superb performance, which can bring about stress and negatively affect security compliance intentions.

Thus, this research attempts to turn attention to the daily circumstances of all employees in present day, struggling with ever-evolving information technology and juggling multiple roles due to information security requirements. Furthermore, we attempt to explore the possibility that new and complex technology and systems that are adopted as security measures in order to improve information security pose additional challenges and burdens on the employees, ironically affecting their information security compliance in an adverse way.

Based on stress theory, this study attempted to pursue the following research objectives: (1) introduce the concept of technostress and role stress to understand the circumstances and experiences of employees in an organization in relation to information security; (2) test how employees' experiences relate to technostress creators and how resultant role stress affects their compliance intention through organizational commitment; and finally; (3) explore a moderating variable determining the strength of the relationship between technostress creators and role stress. In particular, we suggest regulatory focus (i.e., promotion focus and prevention focus) as a potential moderator.

2.1. Technostress and technostress creators related to information security

Since psychologist Craig Brod (1984) introduced the concept of “technostress,” which is a type of stress “caused by an inability to cope with the new computer technology” (p. 16), this term has been expanded to include a specific type of stress experienced by users in organizations related to the use of ICTs. It is usually defined as stress “caused by an individual's attempts to deal with constantly evolving ICTs and the changing physical, social, and cognitive responses demanded by their use (Brillhart, 2004; Clark & Kalin, 1996; Ragu-Nathan, Tarafdar, Ragu-Nathan, & Tu, 2008; Weil & Rosen, 1997). In a situation where information technology is continuously changing, employees tend to feel more stressed (Tarafdar, Bolman Pullins, & Ragu-Nathan, 2014) and experience negative consequences such as dissatisfaction, fatigue, anxiety, overwork, and decreased productivity (Salanova, Llorens, & Cifre, 2013).

Technostress also matters in the context of information security. Organizations require their employees to clearly understand and use the information security technology that they have invested in. Moreover, in order to effectively prevent and control security threats, organizations should impose and practice a strict security policy (Guo & Yuan, 2012; Johnston & Warkentin, 2010). Accordingly, D'Arcy, Herath, & Shoss (2014) introduced the term “Security Related Stress (SRS)” to describe the psychological stress caused by internal or external security-related demands taxing one's cognitive resources or abilities.

Many studies have used the concept of “technostress creators,” i.e., factors that create technostress in an organization due to a mismatch between organizational and individual demands to determine when people feel strain due to technology and experience negative consequences in organizations. Tarafdar et al. (2007) first identified five technostress creators: techno-overload, techno-invasion, techno-insecurity, techno-complexity, and techno-uncertainty. Techno-overload refers to the degree of increase in the amount of work, change in working habits, and demand for faster work performance. Techno-invasion refers to the degree of invasion of an individual's private life by making him or her invest time to learn new technology. Techno-insecurity refers to situations in which users feel threatened about losing their jobs either to automation resulting from new technology or to other people who have a better understanding of the technology. Techno-complexity refers to the inherent quality of information technology that makes employees feel incompetent. Finally, techno-uncertainty refers to the uncertainty of technology due to constant change and upgrades in computer hardware and software. Technostress creators have been used in various contexts to understand which aspects of technology affect employees (Fuglseth & Sørebø, 2014; Jena, 2015; Lee, Son, & Kim, 2016; Ragu-Nathan et al., 2008; Tarafder, Tu, Ragu-Nathan, & Ragu-Nathan, 2011).

Previous research has suggested that employees' stress is a potential cause for employees to avoid participating in organizational goals, resulting in a decrease in individual task and organizational performance (Leung, Shan Isabelle Chan, & Dongyu, 2011; Tziner, Rabenu, Radomski, & Belkin, 2015). Following this line of thought, it is likely that organizational circumstances that pressure employees to adapt to difficult and complex information security procedures and technology may create technostress, which in turn leads to decreased compliance regarding organizational security demands (D'Arcy et al., 2014). We suggest that the influence of technostress creators on information security compliance will be mediated by organizational commitment.

2.2. Organizational commitment and security-related technostress creators

Organizational commitment is defined as an employee's understanding and accepting of organizational goals and values, and forming an identification with the organization (Mowday, Porter, & Steers, 1982; Steers, 1977; Williams & Anderson, 1991). Organizational commitment induces voluntary behaviors from employees that benefit peers and the organization. People with strong organizational commitment tend to have a high degree of devotion