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/

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

towards the organization (Meyer, Stanley, Herscovitch, & Topolnytsky, 2002), subsequently focusing on achieving positive results in the organization (Allen & Meyer, 1996; Murrell & Sprinkle, 1993).

For many employees, information security may not be their primary goal. Sometimes, information security may even hinder employees from achieving their individual goals since security compliance requires additional work processes or conflicts with their task requirements. Under these circumstances, employees may violate information security when the benefit of compliance is lower than the cost of compliance (Bulgurcu et al., 2010). Since organizational commitment involves accepting organizational goals and values, it is possible that organizational commitment makes employees accept the necessity of information security (Stanton, Stam, Guzman, & Caldera, 2003) and pursue it as an organizational goal. In other words, organizational commitment can work as an antecedent for employees to overcome the inconvenience of information security compliance and to give employees the perception that information security compliance is necessary.

Consistent with this reasoning, it is suggested that organizational commitment is associated with information security compliance. Stanton et al. (2003) found that higher organizational commitment increases employee's security compliance. Similarly, Li, Zhang, and Sarathy (2010) showed that employees who identify with the organization have a higher compliance intention with the organization's internet use policy.

It is also suggested that organizational commitment can be influenced by the environmental characteristics of the organization (Lee, Lee, & Yoo, 2004). For example, Meyer (2009) demonstrated that uncertainty and instability of the employees' working environment decreases the employees' organizational commitment, which suggests the possibility that an organization's constantly evolving environment regarding information security technology may work as a factor decreasing employees' organizational commitment. There are several studies that support this reasoning. In a study by Ragu-Nathan et al. (2008), technostress creators were found to decrease employees' job satisfaction and in turn decrease organizational commitment. Similarly, Jena (2015) showed that information technostress creators negatively influence employees' organizational commitment and suggested that organizations can benefit from various employee-supporting systems or programs to mitigate the adverse effect. Based on this reasoning, we propose H1 as follows:

**H1**. Security-related technostress creators reduce employees' intention to comply with their organization's information security through organizational commitment.

- H1a Security-related technostress creators reduce organizational commitment.
- H1b Organizational commitment increases employees' compliance intention.

### 2.3. Role stress related to information security

Role stress is defined as an awareness or feeling of personal dysfunction resulting from perceived conditions or happenings in the workplace and one's psychological and physiological reactions to these uncomfortable, undesirable, or threatening workplace conditions (Jamal, 1990; Parker & DeCotiis, 1983). Two main causes of role stress are role conflict and role ambiguity. Role conflict is the perception of incompatibility in the requirements of the role (Galluch, Grover, & Thatcher, 2015) and occurs when an employee is asked to fulfill an overwhelming amount of tasks by the organization (Tarafdar et al., 2007). Role ambiguity is the unpredictability of the consequences of one's role performance and lack of information needed to perform the role (Ayyagari, Grover, & Purvis, 2011; Behrman & Perreault, 1984).

It is expected that the technological environment regarding information security can be a factor affecting the degree of role conflict and role ambiguity of employees who have to deal with the organization's security requirements and their own job requirements. For most employees, achieving their own job goals is the priority, and complying with information security policy may not be on top of their list. However, organizations require employees to comply with information security, which may not be compatible with employees' job processes. For instance, when achieving one's job goal of finalizing a deal in a timely manner with an external partner that requires exchanging important documents, the security policy imposes complex technological features and procedures that can take days to complete, and the employee will experience a large amount of conflict between his or her individual goal and the security goal. When the purpose and direction of security compliance is poorly aligned with individual goals in an organization and the security requirements tend to impose additional job burdens, role conflict can easily occur between an organization's security requirements and an employee's job requirements (Hu et al., 2011).

In addition, when an organization's security requirement changes based on the development of information security technology, it generally leaves employees with a lack of information and confusion, leading to role ambiguity. For instance, if an organization wants its employees to shift from PCs to mobile devices to perform a job, the information security technology requirement is modified to suit such a change. Employees may not have a clear understanding of the new technology and the information security requirements or resources to get help regarding the change, which may lead to a great level of role ambiguity. Thus, it is highly likely that an organization's technological environment regarding information security and security-related technostress creators can lead to employees' security-related role stress.

Vakola and Nikolaou (2005) indicated that employees' overall occupational stress is negatively related to organizational commitment. Tziner et al. (2015) also showed that role stress increases burnout and intention to leave and decreases job satisfaction, which potentially suggests that it is also associated with decreased organizational commitment. Based on previous literature, we propose hypotheses regarding role stress (H2):

**H2**. The influence of security-related technostress creators on organizational commitment is mediated by security-related role stress.

- H2a Security-related technostress creators directly increase security-related role stress.
- H2b Security-related role stress reduces organizational commitment.

Finally, we attempted to identify an individual difference that moderates the relationship between technostress creators and role stress on the job. We suggest regulatory focus as a moderator.

### 2.4. Regulatory focus as a moderator between technostress creators and role stress

We explored the possibility that employees' responses to technological demands in an organization are affected by their chronic differences in regulatory focus. Regulatory focus theory (Higgins, 1997; Keller, 2006) assumes that there are two distinct types of motivational orientation (promotion focus and prevention focus), which serve fundamentally different needs. People with a

promotion focus orient their experience to meet an "ideal," something that satisfies the need for nurturance and accomplishment, whereas people with a prevention focus orient their experience to fulfill a responsibility or an "ought," something that satisfies the need for security and protection. For example, Gorman, Meriac, Overstreet, Apodaca, McIntyre, Park, and Godbey's (2012) recent meta-analysis on regulatory focus indicated that the promotion focus was positively associated with antecedents such as positive affect, optimism, and learning goal orientation, and negatively associated with anxiety and negative affect, whereas the relationship was significantly different for the prevention focus.

The two different kinds of regulatory focus have been associated with distinct strategic inclination: people with a promotion focus are sensitive to the presence or absence of positive outcomes and approaching matches, whereas people with a prevention focus are sensitive to the presence and absence of negative outcomes and avoiding mismatches (Gino & Margolis, 2011). Researchers have suggested that chronic individual differences in regulatory focus can have important moderating effects in organizational processes. Recently, using a job demands-resources model, Brenninkmeijer, Demerouti, le Blanc, and Hetty van Emmerik (2010) demonstrated that job demands such as interpersonal conflict and work load had a detrimental effect on those with a strong prevention focus; however, job resources such as support from colleagues and autonomy had a beneficial effect on those with a relatively weak promotion focus. In the context of information technology (IT) compliance literature, Liang, Xue, and Wu (2013) found that the positive influence of reward expectancy on IT compliance was stronger for people with a stronger promotion focus, while the positive influence of punishment expectancy on IT compliance was stronger for people with a higher prevention focus.

Few studies have directly examined the role of regulatory focus in the IT compliance literature, and we speculate that employees' chronic level of promotion and prevention focus can affect their responses to security-related technostress creators and their experiences of security-related role stress on the job. Findings regarding regulatory focus suggest the possibility that a stronger promotion focus is associated with active and more effective coping styles for stressful situations, whereas a stronger prevention focus is associated with passive coping styles that lead to a negative response to stressful situations (Brockner & Higgins, 2001; Tamir, 2005; Zhao & Namasivayam, 2012).

Based on these results, the present study hypothesizes that a regulatory focus moderates the relationship between security-related technostress creators and employees' experience of security-related role stress. Specifically, a strong promotion focus helps employees to resist the negative influence of security-related technostress creators and experience less security-related role stress on the job, whereas a strong prevention focus makes people susceptible to experiencing more security-related role stress from security-related technostress creators. These arguments lead to the following hypotheses (H3):

**H3**. The relationship between security-related technostress and role stress is moderated by regulatory focus.

- H3a People with a high promotion focus are less likely to be affected by security-related technostress creators and experience less role stress.
- H3b People with a high prevention focus are more likely to be affected by security-related technostress creators and experience more role stress.

Overall, this research presents how security-related technostress creators (TC) and security-related role stress (RS) might decrease security compliance intention via organizational commitment (See Fig. 1).

## 3. Methods

### 3.1. Participants & procedure

Participants were sampled from 20 large firms in South Korea that comply with IT security standards and apply information security policies at the company level. This study especially targeted participants who had at least five years of job experience at their current position and who had to deal with information security technology and policy as part of their day-to-day tasks but were not members of departments directly responsible for managing the information security of the company.

Of course, employees in the information security departments are the ones who should experience considerable technostress; however, they might not experience too much role stress because their main job is to make sure all security requirements are met, so following security policy does not conflict with their daily routine of work. This may not be the case for other employees, however. As for employees outside of the information security department, complying with the company's information security policy may not be their main goal, and it is likely that unfamiliar information security technology and requirements create various conflicts and uncertainty in achieving their main departmental goal on a daily basis. Thus, this study suggests that the relationship between circumstances that create technostress and security-related role stress are more present in employees outside the information security department and explores whether technostress creators and role stress potentially hamper their intention to comply with information security requirements.

Managers at the 20 firms in finance/insurance, manufacturing, and distribution industries were contacted for permission to conduct the survey on site. The survey questionnaire was distributed and collected either directly at the individual branch offices or indirectly by mail. A total of 658 employees at 55 sites were solicited for the survey. Responses from 379 participants were collected. After excluding data from 33 respondents due to incomplete information, data from a total of 346 participants were used for the analyses.

Of the 346 participants, 56.1% were male; 40.5% were 31–40 years old, and 29.5% 41–50 years old. Most of them were in the finance/insurance industry (68.8%), followed by manufacturing (23.1%) and distribution (8.1%). Finally, most of the participants held the job title of staff member (68.2%), and managers and senior/executive managers consisted of 15.9%, which represented employees at different levels rather accurately. Demographic characteristics of the participants are presented in detail in Table 1.

### 3.2. Measures

The questionnaire contained measures that tap into five main constructs in the proposed model: security-related technostress creators (TC), security-related role stress (RS), regulatory focus, organizational commitment and compliance intention. A detailed description of each is provided in the following section. A complete list of items (with Cronbach's alphas for subscales) are presented in the Appendix.

#### 3.2.1. Security-related technostress creators (TC)

When D'Arcy et al. (2014) coined the term "Security-Related Stress" by applying the concept of technostress creators to the context of security, they used only three of the original five factors: overload, complexity and uncertainty. They excluded invasion and insecurity since they were not appropriate in the context of

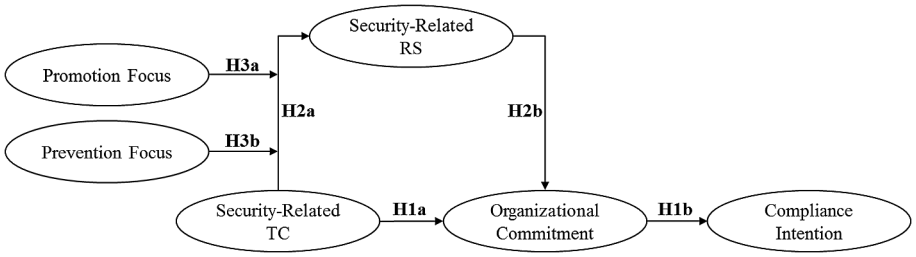


**Fig. 1.** Research model.

**Table 1**
Demographic characteristics of participants.

| Characteristics | | Frequency (%) | |
|---|---|---|---|
| | | 346 | (100.0) |
| Industry | Finance/Insurance | 238 | (68.8) |
| | Manufacturing | 80 | (23.1) |
| | Distribution | 28 | (8.1) |
| Gender | Male | 194 | (56.1) |
| | Female | 152 | (43.9) |
| Age | <30 | 93 | (26.9) |
| | 31–40 | 140 | (40.5) |
| | 41–50 | 102 | (29.5) |
| | >50 | 11 | (3.2) |
| Job Title | Staff | 236 | (68.2) |
| | Manager | 55 | (15.9) |
| | Senior/Executive Manager | 55 | (15.9) |

security. Adopting their approach, this study uses the term security-related technostress creators (TC) to indicate factors that cause technostress in relation to information security technology.

Security-related technostress creators (TC) are defined as the degree of overload, complexity, and uncertainty of information security technology that causes employees psychological stress. First, security-related techno-overload refers to increased workload due to required information security technology. For example, in order to protect documents, employees might have to perform additional work processes. Similarly, employees may be required to get permission from the security department before they exchange documents with external partners.

Second, security-related techno-complexity refers to the degree of complexity of security technology, which is an inherent quality of information security technology that makes employees feel incompetent. Four survey items for security-related techno-overload, three items for security-related techno-uncertainty, and four items for security-related techno-complexity from Ragu-Nathan et al. (2008) were adopted and modified for the context of information security.

Finally, security-related techno-uncertainty refers to the degree of change in the work performed by employees due to constant upgrades in information security technology. Organizations try to change their security technology to better suit requirements for newer security technology environments, which can impose stress on employees.

### 3.2.2. Security-related role stress (RS)

We applied the concept of role stress to the context of information security and came up with "security-related role stress," which is defined as role conflict and role ambiguity that occurs during work due to the requirements of information security.

Security-related role conflict is defined as the degree of contradiction between an individual's effective work procedure and the procedure related to information security technology and the four items from Tarafdar et al. (2007). A sample item reads "I am often asked to do things that are against my better judgment."

Four items from Ayyagari et al. (2011) were used for security-related role ambiguity. A sample item includes "I am unsure what to prioritize: dealing with information security problems or my work activities."

### 3.2.3. Regulatory focus

Two regulatory foci, promotion focus and prevention focus, were measured using the scale by Lockwood, Jordan, and Kunda (2002), which includes six items for each construct. Promotion focus is defined as an employee's intention to integrate him or herself with the goal, and a sample item is "In general, I am focused on achieving positive outcomes in my differing from the goal." A sample item for the prevention focus is "In general, I am focused on preventing negative events in my life." Original items were modified to suit the context of information security, and participants were asked to indicate their answers on a seven-point Likert scale: 1 = strongly disagree to 7 = strongly agree.

### 3.2.4. Organizational commitment

Organizational commitment is defined as the psychological state of employees understanding and forming identification with organizational goals and values. Four items by Herath and Rao (2009) were used in the study, and a sample item is "I really feel as if this organization's problems are my own."

### 3.2.5. Compliance intention

Compliance intention is defined as an employee's intention to protect the organization's information resources. Four items by Chen, Ramamurthy, and Wen (2012) were used. A sample item reads "I am certain that I will follow information security policies."

## 4. Results

### 4.1. Reliability and validity analysis

Table 2 shows the construct items and reliabilities. A reliability analysis was performed using factor loading and Cronbach's alpha. A reliability analysis was performed using 37 out of the 38 total items. RC3 was excluded due to problems in the factor loading value. As a result, Cronbach's alpha of the 9 constructs ranged from 0.854 to 0.949, which met the general criteria of 0.70 (Nunnally, 1978). Information security TC and RS were considered to be second order constructs with items of overload, uncertainty, complexity, role ambiguity, and role conflict, respectively. Table 3 shows the value for Cronbach's alpha of information security TC (0.810) and RS (0.781).

We assessed the convergent and discriminant validity of the measurement model through a second confirmatory factor analysis using AMOS 22.0. In order to control for the demographic characteristics of participants, gender, age, industry, and job title were

**Table 2**
Results for reliability and validity analysis.

| Construct | Item | Mean | Std. Dev. | Factor Loading | Cronbach's Alpha | CR | AVE |
|---|---|---|---|---|---|---|---|
| Security-Related TC[a] | TO | 2.85 | 1.01 | 0.612 | 0.810 | 0.808 | 0.585 |
| | TC | | | 0.628 | | | |
| | TU | | | 0.543 | | | |
| Security-Related RS[a] | RC | 2.77 | 1.11 | 0.822 | 0.782 | 0.769 | 0.625 |
| | RA | | | 0.715 | | | |
| Organizational Commitment | OC1 | 4.91 | 1.03 | 0.830 | 0.910 | 0.895 | 0.681 |
| | OC2 | | | 0.826 | | | |
| | OC3 | | | 0.858 | | | |
| | OC4 | | | 0.812 | | | |
| Compliance Intention | CI1 | 5.61 | 1.12 | 0.893 | 0.949 | 0.958 | 0.851 |
| | CI2 | | | 0.883 | | | |
| | CI3 | | | 0.883 | | | |
| | CI4 | | | 0.830 | | | |
| Promotion Focus | Prom1 | 5.51 | 1.10 | 0.834 | 0.936 | 0.927 | 0.810 |
| | Prom2 | | | 0.866 | | | |
| | Prom3 | | | 0.837 | | | |
| | Prom4 | | | 0.846 | | | |
| | Prom5 | | | 0.850 | | | |
| | Prom6 | | | 0.846 | | | |
| Prevention Focus | Prev1 | 4.38 | 1.28 | 0.756 | 0.854 | 0.786 | 0.552 |
| | Prev2 | | | 0.812 | | | |
| | Prev3 | | | 0.850 | | | |
| | Prev4 | | | 0.827 | | | |
| | Prev5 | | | 0.720 | | | |
| | Prev6 | | | 0.678 | | | |

Note.
[a] Second Order Construct; TO, TC, TU, RC, and RA stand for Techno-Overload, Techno-Complexity, Techno-Uncertainty, Role Conflict, and Role Ambiguity, respectively.

**Table 3**
Results for discriminant validity.

| Construct | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Security-Related TC[a] | **0.765** | | | | | |
| Security-Related RS[a] | 0.510** | **0.791** | | | | |
| Organizational Commitment | −0.606** | −0.570** | **0.825** | | | |
| Compliance Intention | −0.654** | −0.514** | 0.428** | **0.923** | | |
| Promotion Focus | −0.534** | −0.450** | 0.472** | 0.547** | **0.900** | |
| Prevention Focus | −0.195** | −0.104 | 0.170** | 0.153** | 0.242** | **0.743** |

Note. *$p < .05$, **$p < .01$; values in bold type along the diagonal indicate the square root of the AVE.
[a] Second Order Construct.

included in the model as control variables. The overall fitness of the measurement model was examined based on a number of factors, including the relative $\chi^2$ ($\chi^2/df$), the goodness-of-fit index (GFI), the adjusted goodness-of-fit index (AGFI), the comparative fit index (CFI), the normed fit index (NFI), and the root mean square error of approximation (RMSEA). A GFI, NFI, and CFI higher than 0.90 (Bentler, 1990), AGFI higher than 0.8 (Fornell & Larcker, 1981), and RMSEA lower than 0.06 (Jöreskog & Sörbom, 1996) indicate a good fit. In addition, the value of $\chi^2/df$ is expected to range from 3 to 5 (Goodhue, 1995).

The result of the second confirmatory factor analysis showed that all fit indices of the models were appropriate as advised ($\chi^2 = 1.422$, GFI = 0.901, AGFI = 0.880, CFI = 0.982, NFI = 0.944, RMSEA = 0.035). Convergent validity was calculated using the construct reliability (CR) and average variance extracted (AVE). The literature suggests that the reliability of all constructs will be higher than the minimum cutoff score of 0.70 (Wixom & Watson, 2001) and AVE will be higher than 0.5 (Fornell & Larcker, 1981). The construct reliability results ranged from 0.769 to 0.958, and AVE ranged from 0.552 to 0.851. Thus, the convergent validity was considered to be acceptable (See Table 2).

Discriminant validity was checked by examining whether the correlations between the variables were lower than the square root of the AVE (Fornell & Larcker, 1981). The analysis indicated that the correlations between the relevant variables did not exceed the square root of the AVE. The results are demonstrated in Table 3.

The problem of common method bias can be raised since all measures were obtained from a single source with self-reported measures and constructs that showed a relatively high degree of correlation. In order to respond to this problem, we checked whether common method bias poses a serious problem in the study in two ways: Using (1) Harman's (1967) single-factor test and (2) a single-common-method-factor approach (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003).

First, we used Harman's single-factor test and performed exploratory factor analysis (EFA) including all items in this study. EFA assumes that considerable common method variance exists if (1) a single factor emerges from unrotated factor solutions, or (2) a first factor with eigenvalues greater than 1.00 explains a majority of the variance (Podsakoff & Organ, 1986). Exploratory factor analysis on all items revealed nine factors, which explained 41.2% of the variance, but no single factor explained a majority of the variance. Thus, it was inferred that common method bias did not present a significant problem.

Second, we tried another statistical remedy by adopting a single-common-method-factor approach. In this technique, items are allowed to load on their theoretical constructs, as well as on a latent common methods variance factor, and the significance of the

structural parameters is compared both with and without the latent common methods variance factor in the model (Podsakoff et al., 2003). The purpose of this test was to examine whether the estimated parameters in the proposed model were significantly changed after adding a common method factor in the model. The result of this test showed that the common method factor model did improve the goodness-of-fit index ($\chi^2 = 509.0$ ($df = 407$, $p < .01$), GFI = 0.918, AGFI = 0.894, CFI = 0.990, NFI = 0.954, and RMSEA = 0.027) compared to the proposed model without a common method factor ($\chi^2 = 624.3$ ($df = 439$, $p < .01$), GFI = 0.901, AGFI = 0.880, CFI = 0.982, NFI = 0.944, and RMSEA = 0.035), with a significant change of chi-square ($\Delta\chi^2 = 115.3$, $p < .01$) (Williams & Anderson, 1994). However, the goodness of fit indices of the proposed model without the common method factor still demonstrated a good fit, and therefore, based on these two tests, we concluded that common method bias did not present a significant threat to our results.

### 4.2. Structural model

The research hypotheses were examined using structural equation modeling (SEM) with AMOS 22.0. Six common model-fit indices were used to estimate the fit of the measurement model. They satisfied the required level: $\chi^2/df = 2.059$, GFI = 0.901, AGFI = 0.854, CFI = 0.948, NFI = 0.904, and RMSEA = 0.055.

Fig. 2 presents the results of the model testing. First, we attempted to show that security-related technostress creators affected compliance intention through organizational commitment. The analysis demonstrated that security-related technostress creators negatively affected organizational commitment ($\beta = -0.423$, $p < .01$), supporting H1a. Furthermore, analysis of the relationship between organizational commitment and compliance intention demonstrated that organizational commitment had a positive influence on compliance intention ($\beta = 0.490$, $p < .01$), supporting H1b.

We also examined whether role stress mediated the relationship between security-related technostress creators and organizational commitment. The results indicated that security-related technostress creators significantly increased security-related role stress ($\beta = 0.233$, $p < .05$), supporting H2a. In addition, the security-related role stress decreased the organizational commitment ($\beta = -0.490$, $p < .01$), supporting H2b.

The final analysis involved whether regulatory focus moderated the relationship between security-related technostress creators and role stress, i.e., H3a (promotion focus) and H3b (prevention focus). Since there were three security-related technostress creator items and six regulatory focus items, we performed item parceling on the regulatory focus items. Interaction terms were created using the matched-pair strategy suggested by Marsh, Wen, and Hau (2004) and the double mean-centering method suggested by Lin, Wen, Marsh, and Lin (2010). The results showed that the moderation effect regarding the promotion focus was statistically significant ($\beta = -0.168$, $p < .05$), whereas the moderation effect regarding the prevention focus was not ($\beta = -0.126$, $p > .05$). Thus, only hypothesis H3a was supported.

In order to illustrate the moderation effects, simple slopes were plotted following the procedure by Dawson (2014) (See Fig. 3). Two regression lines illustrate the relationship between security-related technostress creators and role stress when the level of regulatory focus is low (one standard deviation below the mean) and high (one standard deviation above the mean). As Fig. 3 shows, the promotion focus moderated the relationship between security-related technostress creators and security-related role stress. Generally, security-related technostress creators increased security-related role stress. However, the negative effect of security-related technostress creators was mitigated for employees with a high level of promotion focus. These employees experienced less security-related role stress, even when they reported that they were in an environment that could potentially create a greater level of security-related technostress. Differences in the prevention focus did not moderate the relationship between security-related technostress and role stress.

Finally, the $R^2$ values of the endogenous variables indicated that organizational commitment, security-related RS and compliance intention explained 68.0%, 38.8%, and 26.0% of the variance, respectively.

## 5. Discussion

### 5.1. Summary of results

The results of this study can be summarized as follows. First, security-related technostress creators negatively affected information security compliance through organizational commitment (H1a and H1b). Second, security-related technostress creators were found to be associated with another type of stress, role stress regarding one's job (H2a), and the increased level of security-related role stress due to security-related technostress creators

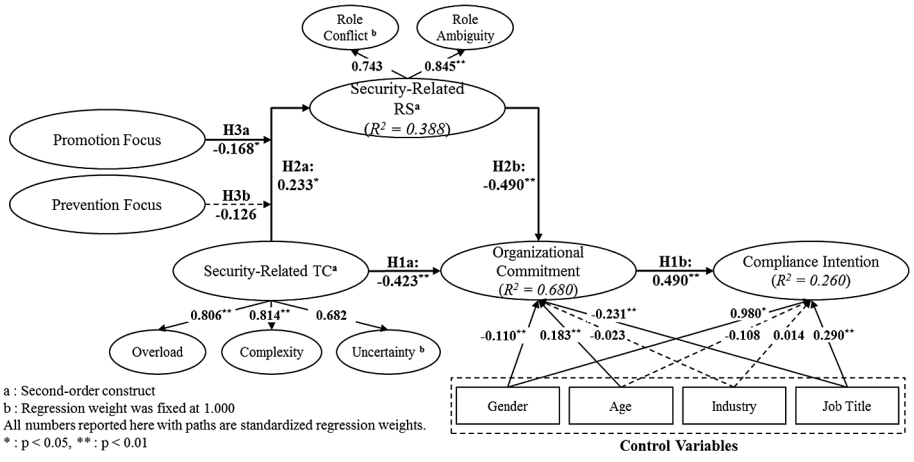


**Fig. 2.** Results of the structural model.

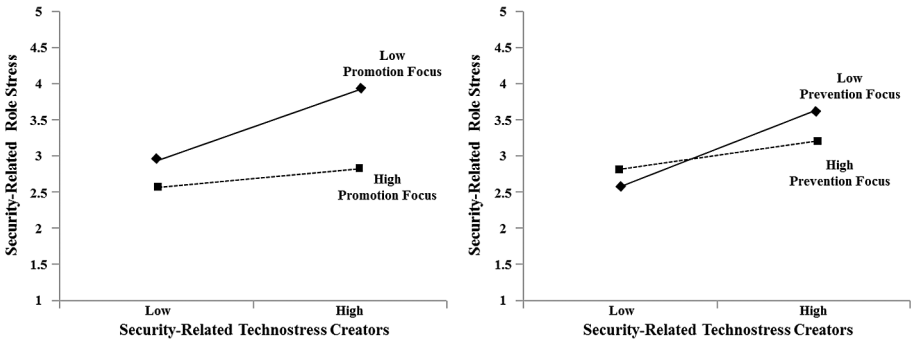


**Fig. 3.** Moderation Effect of Promotion Focus vs. Prevention Focus.

further served as another antecedent to decrease organizational commitment (H2b). Finally, employees' promotion focus significantly influenced how employees responded to security-related technostress creators. Even though security-related technostress creators generally increased security-related role stress, employees with a strong promotion focus experienced less role stress than employees with a weak promotion focus (H3a). However, the prevention focus did not moderate the relationship (H3b not supported).

### 5.2. Theoretical implications

Our study attempted to extend previous research and fill the gap in the information security literature. First, this study tried to provide a theoretical extension of the information security literature by integrating the concept of technostress and role stress. Although it is generally expected that compliance with information security requires knowledge and adjustment to the complex and difficult technology on the part of employees, their experiences of technostress and its potential influence on their attitude regarding information security and security policy have largely been ignored in the information security literature.

D'Arcy et al.'s (2014) study was one of a few studies that introduced the concept of technostress to information security literature. Using the name security-related stress (SRS), they highlighted the importance of technostress and demonstrated the relationship between SRS and information security policy (ISP) violation intention. However, D'Arcy et al. (2014) seemed to focus more on the moral disengagement process as a coping mechanism, and SRS was shown to affect information security policy violation intention only through the moral disengagement as a mediator.

Just as D'Arcy et al. (2014), we acknowledge the fact that stress components due to information security technology should be considered an important factor affecting employees' information security compliance in organizations. However, this study goes further to delineate *how a stress-inducing environment due to broad technology possibly affects the everyday lives of employees on all job levels by adopting the concept of role stress* (Tarafder, Tu, Ragu-Nathan, & Ragu-Nathan, 2007, 2008).

*The findings of our study show that* technostress creators increase role stress on the job, and circumstances regarding information security technology are no exception. As information security technology gets more complex and specialized, employees who have to deal with requirements regarding information security technology in various stages of their job processes are likely to experience an increased level of role conflict and ambiguity.

Second, we suggest that stressors due to information security technology and resultant role stress can negatively affect compliance with information security by harming employees' commitment to their organizational goals. Organizational commitment can be understood as employees' willingness to believe in and to form identification with the organization (Meyer et al., 2002). Employees with a higher level of organizational commitment have a tendency to integrate themselves with the organization's goals (Stanton et al., 2003). This study demonstrates that increasing pressure of security-related technology and an increased level of role stress can serve as important sources to undermine organizational commitment, which in turn distracts employees from focusing on the organization's goal of promoting information security compliance. Using organizational commitment as a mediator, this study suggests that employees' compliance with information security is not just a matter of an individual decision according to employees' own moral standards or their personal analysis of costs and benefits; rather it is a decision involving their relationship with the organization, i.e., whether to identify with the organization and to resonate with its goal regarding information security.

Finally, this study examined the effect of regulatory focus as a potential individual difference that moderates the relationship between security-related technostress creators and security-related role stress. This attempt extends the research by Tarafdar et al. (2007, 2014) and explores the relationship between technostress creators and role stress on a deeper level. Regulatory focus has been investigated extensively in information security literature, usually in terms of how people respond to reward and punishment regarding information security compliance. However, we used regulatory focus as a way to understand and predict how individuals react differently to a stressful environment. Our finding suggests that regulatory focus, especially a promotion focus, seems to be involved in buffering the adverse effects of technostress creators and decreasing role stress. Whether a promotion focus affects the perception of the stressor itself or the adoption of coping styles remains to be answered, which begs an interesting and promising exploration for future studies.

### 5.3. Managerial implications

Findings from this study demonstrate how employees' information security compliance intention can be affected by technostress creators and role stress in relation to information security technology. Although the majority of information security threats come from outside, a rather consistent portion of security breaches and incidents still seems to be coming from insiders. According to the 2017 DBIR (Data Breach Investigations Report) (Verizon, 2017), of 1935 security breaches that occurred in 2016, 75% were perpetrated by outsiders and 25% involved internal actors. The report also

states that security breaches in absolute numbers driven by internal parties, largely consisting of privilege misuse and miscellaneous errors, have remained relatively constant with an increase of around 12% (Verizon, 2017, p. 5). In addition, it should be noted that employees of all levels and positions who have access to and use information systems in organizations are capable of intentionally or unintentionally violating information security (West, 2008). As an illustration, an analysis of 2014 breaches revealed that incident classification such as privilege abuse, which is the defining characteristic of internal actor breach, involved actors ranging from staff at the cash register, call center, or help desk to executives, managers and even system administrators (Verizon, 2015).

The picture seems to suggest that there is always a considerable number of employees at all levels who either intentionally or unintentionally cause security incidents by misusing privilege and by making miscellaneous errors. It seems that most of the resources and efforts are invested in preparing for external attacks and invasion, not investigating the circumstances regarding why employees inside organizations ended up misusing privilege or making errors. In addition, it is largely neglected that protecting an organization by enhancing information security technology might have unexpected results; ever-changing and complex information technology and security procedures might leave people inside the organizations in a stressful situation dealing with overload, information complexity, and a sense of uncertainty.

In this sense, this study provides an initial piece of evidence illustrating how organizations' efforts to enhance information security technology have an ironic effect: it makes the employees' working environment susceptible to technostress and resultant role stress, which in turn unintentionally results in inhibiting their security compliance intention. Appropriate amounts of stress can have a positive effect on employees' work performance. However, many studies point out the adverse effects of overwhelming stress on employees. Various characteristics of technostress regarding information security technology such as overload, complexity, and uncertainty should be further examined to understand their unique impact on employees. Furthermore, our findings imply that organizations should consider managing employees' technostress and role stress regarding information security technology as an essential strategy to improve information security and reduce security breaches and incidents by insider actors.

This study also found that regulatory focus moderated the relationship between security-related technostress creators and security-related role stress of employees. More specifically, security-related technostress creators tended to increase employees' security-related role stress; however, those with a high promotion focus were more resistant to the adverse effects of security-related technostress creators. This result indicates that susceptibility to role stress due to technostress regarding information security technology is dependent on chronic individual differences such as the promotion focus.

This finding suggests that assuming the same level of security-related technostress creators, employees with a high promotion focus would be more resistant to experiencing role stress due to technostress and would respond well to the information security policy. The promotion focus is related to pursuing an 'ideal' and 'desirability of action' with 'why' as the important motivation for behavior, whereas the prevention focus is related to 'risk avoidance' and 'feasibility' with 'how' as the important motivation for behavior (Gino & Margolis, 2011; Liang et al., 2013). It seems that the tendency of employees with a high promotion focus to attend to resources and opportunities rather than to demands and threats helps them have a more optimistic view, explore positive opportunities, and adopt task coping to respond well even in stressful situations.

However, people with a low promotion focus feel more role stress on the job when the requirement and the burden of the technostress creators increases, which means that they should be a potential target of monitoring when information security compliance becomes problematic. Furthermore, this result implies that if an organization attempts to introduce an intervention program to mitigate the negative impact of technostress creators, devising a promotion focus program targeting people with a low promotion focus would improve the effectiveness of the program to improve compliance in general.

### 5.4. Limitations and future research

There are some limitations regarding the findings of this study. First, this study demonstrated how stress related to information security technology ultimately affects employees' compliance intention for information security; however, this study did not directly measure employees' compliance performance or behavior regarding information security. Even though it is plausible to assume that behavioral intention (i.e., compliance intention) can predict actual behavior, future research should consider measuring actual behaviors to clearly establish the relationship between information security-related technostress and information security compliance.

Second, this study focused on potential stress or psychological strain that information security technology imposed on employees as a potential factor affecting their compliance with information security. This study was able to show that technostress creators increase employees' role stress, and the increased level of stress can negatively affect compliance intention through decreased organizational commitment. This finding provides initial evidence on how security-related technostress creators influence security compliance. As our main research question was to establish the relationship between technostress and role stress related to information security technology and security compliance intention in general, we controlled for variables that were irrelevant to our question such as gender, age, job title, and industry. However, the level of requirements for information security technology might be different depending on the type of industry, organization, department, task and relevant culture or norms. Furthermore, whether an employee will experience technostress can be influenced by various individual characteristics such as gender, age, education, experience, training or efficacy regarding using computers and technology (Tarafdar et al., 2011). These variables themselves may pose interesting research questions in terms of how these factors play into the relationship between technostress and security compliance intention. Future research should examine both organizational contexts and individual characteristics that moderate the relationship between information security-related technostress and compliance.

In addition, we speculated that a high promotion focus makes employees less vulnerable to the adverse effects of security-related technostress by making people focus more on rewards and opportunities and adopt more adaptive coping styles to deal with the stressful situation. However, the design of this study was not able to examine the exact process of how promotion focus exerts a mitigating effect. Future research should attempt to understand the process of how regulatory focus affects the influence of technostress creators on compliance intention.

### 5.5. Conclusions

In sum, this study provides the following insights. First, security-related technostress creators and security-related role stress are important antecedents affecting employees' security

compliance. This study suggests the importance of managing employees' stress as an important source of threat to information security technology in organizations. Second, security-related technostress creators and security-related role stress negatively affect compliance intention through organizational commitment. Therefore, this study presents the importance of organizational commitment in predicting and enhancing employees' security compliance intention. Finally, the strength of employees' security-related role stress due to security-related technostress creators is determined by their individual level of promotion focus. This suggests that understanding individual differences between employees, such as a chronic level of promotion focus, is important for monitoring and managing information security compliance as well as stress in organizations.

## Acknowledgement

I. Hwang was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea [NRF-2016S1A5A8019240].

## Appendix. Item Descriptions with Reliabilities

| Constructs | | Items # | Items |
|---|---|---|---|
| Security-Related Technostress Creators (TC) | Techno-Overload (Ragu-Nathan et al., 2008) $\alpha$=0.909 | STO1 | I am forced by information security technology to work much faster. |
| | | STO2 | I am forced by information security technology to do more work than I can handle. |
| | | STO3 | I am forced by information security technology to work with very tight time schedules. |
| | | STO4 | I am forced to change my work habits to adapt to new information security technology. |
| | Techno-Complexity (Ragu-Nathan et al., 2008) $\alpha$=0.903 | STC1 | I do not know enough about information security technology to handle my job satisfactorily. |
| | | STC2 | I need a long time to understand and use new information security technologies. |
| | | STC3 | I do not have enough time to study and upgrade my information security technology skills. |
| | | STC4 | I often find it too complex for me to understand and use new information security technologies. |
| | Techno-Uncertainty (Ragu-Nathan et al., 2008) $\alpha$=0.936 | STU1 | There are always new developments in the information security technology we use in our organization. |
| | | STU2 | There are frequent upgrades to information security technologies in my organization. |
| | | STU3 | There are always new information security requirements in my job. |
| Security-Related Role Stress (RS) | Role Conflict (Tarafdar et al., 2007) $\alpha$=0.920 | RC1 | I am often asked to do things that are against my better judgment. |
| | | RC2 | I often receive assignments without adequate resources and materials to execute them. |
| | | RC3 | I often have to bend rules or policy in order to carry out an assignment. |
| | | (Drop) | |
| | | RC4 | I often receive incomplete requests from two or more people. |
| | Role Ambiguity (Ayyagari et al., 2011) $\alpha$=0.936 | RA1 | I am unsure whether I have to deal with information security problems or with my work activities. |
| | | RA2 | I am unsure what to prioritize: dealing with information security problems or my work activities. |
| | | RA3 | I cannot allocate time properly for my work activities because my time spent on information security activities varies. |
| | | RA4 | Time spent resolving information security problems takes time away from fulfilling my work responsibilities. |
| Organizational Commitment (Herath & Rao, 2009) $\alpha$=0.910 | | OC1 | I would be happy to spend the rest of my career in this organization. |
| | | OC2 | I enjoy discussing my organization with people outside it. |
| | | OC3 | I really feel as if this organization's problems are my own. |
| | | OC4 | This organization has a great deal of personal meaning for me. |
| Compliance Intention (Chen et al., 2012) $\alpha$=0.949 | | CI1 | It is possible that I will follow information security policies. |
| | | CI2 | It is probable that I will follow information security policies. |
| | | CI3 | I am likely to follow information security policies. |
| | | CI4 | I am certain that I will follow information security policies. |
| Regulatory Focus | Promotion Focus (Lockwood et al., 2002) $\alpha$=0.936 | Prom1 | I frequently imagine how I will achieve my hopes and aspirations. |
| | | Prom2 | I often think about the person I would ideally like to be in the future. |
| | | Prom3 | I typically focus on the success I hope to achieve in the future. |
| | | Prom4 | I see myself as someone who is primarily striving to reach my "ideal self"—to fulfill my hopes, wishes, and aspirations. |
| | | Prom5 | In general, I am focused on achieving positive outcomes in my life. |
| | | Prom6 | I often imagine myself experiencing good things that I hope will happen to me. |
| | Prevention Focus (Lockwood et al., 2002) $\alpha$=0.854 | Prev1 | I frequently think about how I can prevent failures in my life. |
| | | Prev2 | I often think about the person I am afraid I might become in the future. |
| | | Prev3 | I am anxious that I will fall short of my responsibilities and obligations. |
| | | Prev4 | I see myself as someone who is primarily striving to become the self I "ought" to be—to fulfill my duties, responsibilities, and obligations. |
| | | Prev5 | In general, I am focused on preventing negative events in my life. |
| | | Prev6 | I often imagine myself experiencing bad things that I fear might happen to me. |

## References


Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T.

Allen, N. J., & Meyer, J. P. (1996). Affective, continuance, and normative commitment to the organization: An examination of construct validity. *Journal of Vocational Behavior, 49*(3), 252–276. https://doi.org/10.1006/jvbe.1996.0043.

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. *MIS Quarterly, 35*(4), 831–858.

Behrman, D., & Perreault, W. D., Jr. (1984). A role stress model of the performance and satisfaction of industrial salespersons. *Journal of Marketing, 48*(4), 9–21. https://doi.org/10.2307/1251506.

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin, 107*(2), 238–246. https://doi.org/10.1037/0033-2909.107.2.238.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 34*(3), 523–548. https://ssrn.com/abstract=2607190.

Brenninkmeijer, V., Demerouti, E., le Blanc, P. M., & Hetty van Emmerik, I. J. (2010). Regulatory focus at work: The moderating role of regulatory focus in the job demands-resources model. *Career Development International, 15*(7), 708–728. https://doi.org/10.1108/13620431011094096.

Brillhart, P. E. (2004). Technostress in the workplace: Managing stress in the electronic workplace. *Journal of American Academy of Business, 5*(1/2), 302–307.

Brockner, J., & Higgins, E. T. (2001). Regulatory focus theory: Implications for the study of emotions at work. *Organizational Behavior and Human Decision Processes, 86*(1), 35–66. https://doi.org/10.1006/obhd.2001.2972.

Brod, C. (1984). *Technostress: The human cost of the computer revolution*. Reading, MA: Addison-Wesley.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157–188. https://doi.org/10.2753/MIS0742-1222290305.

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perception and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly, 40*(1), 205–222.

Clark, K., & Kalin, S. (1996). Technostressed out? How to cope in the digital age. *Library Journal, 121*(13), 30–32.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210.

Dawson, J. F. (2014). Moderation in management research: What, why, when and how. *Journal of Business and Psychology, 29*(1), 1–19. https://doi.org/10.1007/s10869-013-9308-7.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.2307/3151312.

Fuglseth, A. M., & Sørebø, Ø. (2014). The effects of technostress within the context of employee use of ICT. *Computers in Human Behavior, 40*, 161–170. https://doi.org/10.1016/j.chb.2014.07.040.

Galluch, P. S., Grover, V., & Thatcher, J. B. (2015). Interrupting the workplace: Examining stressors in an information technology context. *Journal of the Association for Information Systems, 16*(1), 1–47.

Gino, F., & Margolis, J. D. (2011). Bringing ethics into focus: How regulatory focus and risk preferences influence (un) ethical behavior. *Organizational Behavior and Human Decision Processes, 115*(2), 145–156. https://doi.org/10.1016/j.obhdp.2011.01.006.

Goodhue, D. L. (1995). Understanding user evaluations of information systems. *Management Science, 41*(12), 1827–1844. https://doi.org/10.1287/mnsc.41.12.1827.

Gorman, C. A., Meriac, J. P., Overstreet, B. L., Apodaca, S., McIntyre, A. L., Park, P., et al. (2012). A meta-analysis of the regulatory focus nomological network: Work-related antecedents and consequences. *Journal of Vocational Behavior, 80*(1), 160–172. https://doi.org/10.1016/j.jvb.2011.07.005.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32*, 242–251. https://doi.org/10.1016/j.cose.2012.10.003.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management, 49*(6), 320–326. https://doi.org/10.1016/j.im.2012.08.001.

Harman, H. H. (1967). *Modern factor analysis*. University of Chicago Press.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005.

Higgins, E. T. (1997). Beyond pleasure and pain. *American Psychologist, 52*(12), 1280–1300. https://doi.org/10.1037/0003-066X.52.12.1280.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54–60. https://doi.org/10.1145/1953122.1953142.

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review, 41*(1), 2–18. https://doi.org/10.1108/OIR-11-2015-0358.

IDC. (2016). *Worldwide semiannual security spending guide*.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007.

Jamal, M. (1990). Relationship of job stress and Type-A behavior to employees' job satisfaction, organizational commitment, psychosomatic health problems, and turnover motivation. *Human Relations, 43*(8), 727–738. https://doi.org/10.1177/001872679004300802.

Jena, R. K. (2015). Technostress in ICT enabled collaborative learning environment: An empirical study among Indian academician. *Computers in Human Behavior, 51*, 1116–1123. https://doi.org/10.1016/j.chb.2015.03.020.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566. http://www.jstor.org/stable/25750691.

Jöreskog, K. G., & Sörbom, D. (1996). *PRELIS 2 User's reference guide: A program for multivariate data screening and data summarization: A preprocessor for LISREL*. Scientific Software International.

Keller, P. A. (2006). Regulatory focus and efficacy of health messages. *Journal of Consumer Research, 33*(1), 109–114. https://doi.org/10.1086/504141.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707–718. https://doi.org/10.1016/j.im.2003.08.008.

Lee, A. R., Son, S. M., & Kim, K. K. (2016). Information and communication technology overload and social networking service fatigue: A stress perspective. *Computers in Human Behavior, 55*, 51–61. https://doi.org/10.1016/j.chb.2015.08.011.

Leung, M. Y., Shan Isabelle Chan, Y., & Dongyu, C. (2011). Structural linear relationships between job stress, burnout, physiological stress, and performance of construction project managers. *Engineering Construction and Architectural Management, 18*(3), 312–328. https://doi.org/10.1108/09699981111126205.

Liang, H., Xue, Y., & Wu, L. (2013). Ensuring employees' IT compliance: Carrot or stick? *Information Systems Research, 24*(2), 279–294. https://doi.org/10.1287/isre.1120.0427.

Lin, G. C., Wen, Z., Marsh, H. W., & Lin, H. S. (2010). Structural equation models of latent interactions: Clarification of orthogonalizing and double-mean-centering strategies. *Structural Equation Modeling, 17*(3), 374–391. https://doi.org/10.1080/10705511.2010.488999.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635–645. https://doi.org/10.1016/j.dss.2009.12.005.

Lockwood, P., Jordan, C. H., & Kunda, Z. (2002). Motivation by positive or negative role models: Regulatory focus determines who will best inspire us. *Journal of Personality and Social Psychology, 83*(4), 854–864. https://doi.org/10.1037/0022-3514.83.4.854.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9.

Marsh, H. W., Wen, Z., & Hau, K. T. (2004). Structural equation models of latent interactions: Evaluation of alternative estimation strategies and indicator construction. *Psychological Methods, 9*(3), 275–300. https://doi.org/10.1037/1082-989X.9.3.275.

Meyer, J. P. (2009). Commitment in a changing world of work. In H. J. Klein, T. E. Becker, & J. P. Meyer (Eds.), *Commitment in organizations* (pp. 37–68). New York: Routledge.

Meyer, J. P., Stanley, D. J., Herscovitch, L., & Topolnytsky, L. (2002). Affective, continuance, and normative commitment to the organization: A meta-analysis of antecedents, correlates, and consequences. *Journal of Vocational Behavior, 61*(1), 20–52. https://doi.org/10.1006/jvbe.2001.1842.

Mowday, R., Porter, L., & Steers, R. (1982). *Employee-organizational linkages: The psychology of commitment, absenteeism and turnover*. New York: Academic Press.

Murrell, A. J., & Sprinkle, J. (1993). The impact of negative attitudes toward computers on employees' satisfaction and commitment within a small company. *Computers in Human Behavior, 9*(1), 57–63. https://doi.org/10.1016/0747-5632(93)90021-J.

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

Parker, D. F., & DeCotiis, T. A. (1983). Organizational determinants of job stress. *Organizational Behavior & Human Performance, 32*(2), 160–177. https://doi.org/10.1016/0030-5073(83)90145-9.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management, 12*(4), 531–544. https://doi.org/10.1177/014920638601200408.

Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., & Tu, Q. (2008). The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information Systems Research, 19*(4), 417–433. https://doi.org/10.1287/isre.1070.0165.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803.

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology: A Sourcebook*, 153–176.
Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012.
Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442–451. https://doi.org/10.1016/j.chb.2015.12.037.
Salanova, M., Llorens, S., & Cifre, E. (2013). The dark side of technologies: Technostress among users of information and communication technologies. *International Journal of Psychology, 48*(3), 422–436. https://doi.org/10.1080/00207594.2012.680460.
Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security, 22*(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045.
Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296–302. https://doi.org/10.1016/j.im.2011.07.002.
Stanton, J. M., Stam, K. R., Guzman, I., & Caldera, C. (2003). Examining the linkage between organizational commitment and information security. In *IEEE international conference on systems man and cybernetics* (Vol. 3, pp. 2501–2506). https://doi.org/10.1109/ICSMC.2003.1244259.
Steers, R. M. (1977). Antecedents and outcomes of organizational commitment. *Administrative Science Quarterly, 22*(1), 46–56. https://doi.org/10.2307/2391745.
Tamir, M. (2005). Don't worry, be happy? Neuroticism, trait-consistent affect regulation, and performance. *Journal of Personality and Social Psychology, 89*(3), 449–461. https://doi.org/10.1037/0022-3514.89.3.449.
Tarafdar, M., Bolman Pullins, E., & Ragu-Nathan, T. S. (2014). Examining impacts of technostress on the professional salesperson's behavioral performance. *Journal of Personal Selling and Sales Management, 34*(1), 51–69. https://doi.org/10.1080/08853134.2013.870184.
Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007). The impact of technostress on role stress and productivity. *Journal of Management Information Systems, 24*(1), 301–328. https://doi.org/10.2753/MIS0742-1222240109.
Tarafdar, M., Tu, Q., Ragu-Nathan, T. S., & Ragu-Nathan, B. S. (2011). Crossing to the dark side: Examining creators, outcomes, and inhibitors of technostress. *Communications of the ACM, 54*(9), 113–120. https://doi.org/10.1145/1995376.1995403.
Tziner, A., Rabenu, E., Radomski, R., & Belkin, A. (2015). Work stress and turnover intentions among hospital physicians: The mediating role of burnout and work satisfaction. *Journal of Work and Organizational Psychology, 31*(3), 207–213. https://doi.org/10.1016/j.rpto.2015.05.001.
Vakola, M., & Nikolaou, I. (2005). Attitudes towards organizational change: What is the role of employees' stress and commitment? *Employee Relations, 27*(2), 160–174. https://doi.org/10.1108/01425450510572685.
Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3), 190–198. https://doi.org/10.1016/j.im.2012.04.002.
Verizon. (2015). *Verizon 2015 data breach Investigations report*.
Verizon. (2017). *Verizon 2017 data breach Investigations report*.
Weil, M. M., & Rosen, L. D. (1997). *Technostress: Coping with technology @work, @home, @play*. New York, NY: Wiley.
West, R. (2008). The psychology of security. *Communications of the ACM, 51*(4), 34–40. https://doi.org/10.1145/1330311.1330320.
Williams, L. J., & Anderson, S. E. (1991). Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. *Journal of Management, 17*(3), 601–617. https://doi.org/10.1177/014920639101700305.
Williams, L. J., & Anderson, S. E. (1994). An alternative approach to method effects by using latent-variable models: Applications in organizational behavior research. *Journal of Applied Psychology, 79*(3), 323–331. https://doi.org/10.1037/0021-9010.79.3.323.
Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication, 1*(4), 317–342. https://doi.org/10.1080/108107396127988.
Wixom, B. H., & Watson, H. J. (2001). An empirical investigation of the factors affecting data warehousing success. *MIS Quarterly, 25*(1), 17–41. https://doi.org/10.2307/3250957.
Zhao, X., & Namasivayam, K. (2012). The relationship of chronic regulatory focus to work-family conflict and job satisfaction. *International Journal of Hospitality Management, 31*(2), 458–467. https://doi.org/10.1016/j.ijhm.2011.07.004.