Exploring the role of intrinsic motivation in ISSP compliance: enterprise digital rights management system case

Soohyun Jeon
Bang College of Business, KIMEP University, Almaty, Kazakhstan
Insoo Son
Department of Global Business Administration, Sangmyung University, Seoul, Korea, and
Jinyoung Han
Chung-Ang University, Seoul, Korea

Received 31 May 2018
Revised 14 February 2019
3 October 2019
Accepted 21 March 2020

Abstract

Purpose – Employee compliance with information system security policies (ISSPs) has been emphasized as a key factor in protecting information assets against insider threats. Even though previous studies have identified extrinsic factors (in the form of external pressure, rewards and social norms) influencing employee compliance, the functioning of employees' intrinsic motivation has not been clearly analyzed. Thus, the aim of this study is to explore the influence of intrinsic motivations on employees' ISSP compliance.

Design/methodology/approach – This study follows a survey approach and conducts structural equation modeling using WarpPLS 5.0 to test the research model and hypotheses. The survey respondents are users of an enterprise digital rights management (EDRM) system.

Findings – The analysis results demonstrate that work impediments, perceived responsibility and self-efficacy significantly influence the intention to comply with ISSP. Additionally, autonomy significantly affects self-efficacy and perceived responsibility. Furthermore, autonomy plays a moderating role in the relationship between work impediment and ISSP compliance intentions.

Originality/value – This study initiatively explores the effect of intrinsic motivations on ISSP compliance intention of employees for a specific information security system (i.e. the EDRM system). This study clarifies the enabling role of intrinsic motivations in ISSP compliance and helps organizations to understand that employee's self-motivated intention, i.e. autonomy, is an essential factor that achieves a higher level of ISSP compliance in the workplace.

Keywords Autonomy, Self-efficacy, Enterprise digital rights management system, EDRM, Information security system policy, ISSP, Policy compliance, Responsibility

Paper type Research paper

1. Introduction

As the value of information assets that affect business success increases, organizations have employed comprehensive protection systems to regulate and secure the use of information systems by employees through an information system security policy (ISSP) (Dhillon, 2007). ISSP prescribes the access controls and authentication processes that allow employees to utilize proper information according to their jobs and positions. Organizations encourage employees to follow the ISSP to maintain business information and knowledge at higher security levels. In many (or most) cases, organizations adopt a command-and-control based security policy to regualte employees' security practices in an efficient and effective manner.

The regulation-based ISSP requires employees to comply with an organization's security rules and motivates them through sanctions and rewards based on their security compliance actions. Despite organizational systems and efforts to prevent information security breaches, many organizations have failed to enforce employee compliance with ISSP. For example, a

Information Technology & People
Vol. 34 No. 2, 2021
pp. 599-616
© Emerald Publishing Limited
0959-3845
DOI 10.1108/ITP-05-2018-0256

survey of insider threat (desk-based workers in the UK and USA) indicates that 49 percent of the 2,000 respondents shared their login ID and password with others to complete their tasks [1]. This result implies that information security regulation may not be sufficiently effective because employees in organizations circumvent ISSP, which is likely to result in severe costs to organizations if unauthorized employees access sensitive data (Ayyagari, 2012). Previous studies on employees' motivations to comply with ISSPs indicate that the effects of extrinsic motivations, such as rewards, external compulsion and social norms, on ISSP compliance have yielded mixed results (Liang *et al.*, 2013; Siponen *et al.*, 2014). Individuals tend to react negatively to an imposed security regulation because they wish to restore their restricted behavioral freedom (Hovav and Putri, 2016). This implies that external control based on regulations is likely to cause a retrograde effect. Thus, information security studies focused on extrinsic motivations have provided limited understanding of why and how employees follow organizational rules to comply with ISSP. To enrich understanding related to security policies, this study proposes intrinsic motivation as an alternative perspective on employees' compliance with ISSP.

The intrinsic motivation perspective suggests that self-motivated employees inspired by personal norms and moral beliefs may better comply with organizations' ISSP because these individuals perceive legitimacy and value congruence between their rule-following actions and organizational security goals as a higher degree (Deci and Ryan, 1987; Son, 2011). Accordingly, this study aims to investigate the effect of employees' intrinsic motivations on ISSP compliance by building a research model and empirically examining the proposed hypotheses through the model. Based on the intrinsic motivation perspectives, the research model developed for this study articulates how autonomy, a self-determining propensity of action, affects the intention to comply with ISSP via self-efficacy and perceived responsibility, which are the antecedents to ISSP compliance intention (LaRose *et al.*, 2008; Wall *et al.*, 2013), and are influenced by autonomy (Sousa *et al.*, 2012; Deci *et al.*, 1994). The research model for this study also considers the moderating role of autonomy between work impediment and ISSP compliance intention. Previous studies indicate that employees do not comply with ISSP because they perceive it as time-consuming, inconvenient or inflexible (Alter, 2014; Ferneley and Sobreperez, 2006; Morin and Pawlak, 2007). For example, mismatches between ISSP and operating procedures (such as system workflows) can result in employees' noncompliance behavior because employees perceive ISSP to be time-consuming and inconvenient with regard to the completion of their tasks. From this perspective, the proposed research model examines whether self-determining behavior such as autonomy attenuates the negative impact of work impediment on ISSP compliance intention. In summary, this study addresses the following two major research questions (RQs):

RQ1. Do intrinsic motivations of employees positively affect ISSP compliance?

RQ2. Does autonomy moderate the relationship between work impediment and ISSP compliance?

To answer these questions, this study is conducted in the context of an enterprise digital rights management (EDRM) system. EDRM is an information security system that protects organizational data through file encryption, permission control and audit trail technologies. Regarding ISSP, an EDRM system contains a set of predetermined rules and permissions, and such EDRM rules are managed by a system administrator. The major functionalities of EDRM systems facilitate logging of content usage, watermarking, assignment of rights per document and user and limiting document usage. Although EDRM systems offer a comprehensive technical environment that enables a higher organization-wide level of information security, employees generally perceive the utilization of an EDRM system to be inconvenient and time-consuming and commit noncompliance actions (Jeon *et al.*, 2018). Such a dual aspect of EDRM operations could provide a proper research setting to explore the role of intrinsic motivation in ISSP compliance.

Next, the research background is first provided, followed by a description of the research model and presentation of the hypotheses. Subsequently, data collection and details of analysis methods are presented. Discussions of the implications of the study, limitations and future research directions conclude this manuscript.

2. Research background

2.1 Intrinsic motivation and information system security compliance

The social psychology literature on human behavior has often explained employees' propensity to follow organizational rules based on two motivation models (Tyler and Blader, 2005). One is an extrinsic motivation model, which focuses on the perceived consequences, such as punishment or reward for breaking or obeying the rules. The other is an intrinsic motivation model, which holds that employees follow the rules because of their innate desires. The extrinsic motivation model has been predominantly used to understand employees' compliance with ISSP. Using the extrinsic model, organizations rely on command-and-control based security policies, stating that noncompliance will result in disciplinary actions, including the termination of employment. In comparison, the intrinsic motivation model of human behavior suggests that employees' innate preferences and desires to follow organizational rules outweigh expected disciplinary outcomes such as rewards and sanctions. Given that the intrinsic motivation model of ISSP is based on a self-regulatory approach, the level of intrinsic motivation to follow rules depends on each employee's personal norms and moral beliefs (Tyler and Blader, 2005). A few studies have offered empirical evidence indicating that employee's moral commitment has a strong deterrent effect on information system (IS) misuse (e.g. D'Arcy *et al.*, 2009). Employees' assessment of their employer is also an important source of the intrinsic motivation to follow workplace rules.

The self-regulatory approach, likened to intrinsic motivation, emphasizes an individual's innate preferences and desires as the fundamental drivers of compliance behavior. Regarding ISSP compliance, previous studies have suggested that employees play a positive key role in maintaining secure IS (Bulgurcu *et al.*, 2010; Crossler *et al.*, 2013), while other studies have identified employees as a weak link in securing organizational information and IS (Warkentin *et al.*, 2011; Willison and Warkentin, 2009). Employees' failure to follow ISSP can be costly to organizations and will cause organizations to implement related command-and-control policies to promote secure behavior. Employees' voluntary execution of positive security behavior is, thus, an essential element that leads to efficient and effective ISSP operation. In line with this, the self-determination perspective provides a useful theoretical view to understand employees' intrinsically motivated behavior to follow organizational ISSP.

Self-determination emerges from the self-determination theory and refers to individuals' belief that their actions are self-guided and drawn from considerate thought, reflection, and choice (Pavey and Sparks, 2009; Ryan and Deci, 2000). The self-determination perspective suggests that autonomy is a fundamental driver of intrinsically motivated behavior. Autonomy refers to individuals' needs and efforts to feel that they direct their own courses of actions and can choose their own behavior. In the ISSP context, autonomy refers to individuals' perception of their abilities to decide whether to voluntarily follow ISSP through their own thoughts and judgments. Research on self-determination suggests that autonomy increases intrinsic motivation. Ryan and Deci (1985), for example, found that individuals are more likely to complete tasks when they have high levels of autonomy. Deci *et al.* (1994) found that individuals with high autonomous orientation are more likely to identify the value of an action and take full responsibility for performing it. In IS research, Ke *et al.* (2012) used the self-determination perspective to examine the influence of intrinsic motivation on the adoption and exploration of enterprise IS. Ke and Zhang (2010) examined the moderating role of self-determination between the motivation and task effort to develop open-source software. Prior studies argue that self-determination perspectives such as autonomy provide a useful research foundation to examine employees' compliance behavior from the intrinsic motivation perspective.

Previous studies also found that employees perceive the requirements of ISSP as costs toward compliance (Bulgurcu *et al.*, 2010). Given that ISSP compliance may require an employee to perform certain activities, such as authentication or approval, the requirements may hinder primary business goals (Pahnila *et al.*, 2007; West, 2008). Thus, employees often perceive the requirements and procedures specified by the ISSP as burdensome and as a barrier to productivity. In line with this, our research model incorporates work impediments arising from the use of EDRM as a factor discouraging ISSP compliance (Alter, 2014). Additionally, this study investigates the moderating role of autonomy, which lessens the negative effect of work impediment on ISSP compliance from the self-determination perspective (Jeon *et al.*, 2018).

2.2 Enterprise digital rights management system

An EDRM system is an example of information security system that supports the prevention of organizational information asset breaches. An EDRM system is also referred to as an information rights management or digital rights management system. Unlike peripheral security methods [2] such as firewalls, EDRM systems focus on the data, wherein the data reside inside or outside an organization (Hennessy *et al.*, 2009). The role of EDRM is to protect organizational data through file encryption, permission control and audit trail technologies. Because of its persistent information asset protection, EDRM systems have become an important tool for securing information assets in the enterprise sector (Morin and Hovav, 2012). EDRM has traditionally employed a control-based ISSP, which contains a set of predetermined rules and permissions; furthermore, EDRM systems are governed by a system administrator. When employees must perform tasks outside their current permissioned level, they are required to request an ISSP adjustment from a supervisor or an administrator. Thus, an EDRM system is a set of tools and methods used to regulate access to information assets. For this study, a security-related task [3] is defined as an employee's task that is fulfilled through an EDRM system.

Employees with the proper rights already granted can immediately complete a security-related task, whereas employees without access rights require an administrative override. The security administrator or supervisor can decide on employee override access rights. Employees cannot complete a task until a supervisor approves their override request. Therefore, employees are likely to stop their assigned task (Figure 1).

As shown in Figure 1, the need for permission of access rights results in inconvenience when it comes to completing an assigned task. As a result, employees attempt to bypass or circumvent the EDRM rules (i.e. ISSP) (Ferneley and Sobreperez, 2006; Alter, 2014). Overall, EDRM systems establish a proper research context for this study wherein intrinsic motivation factors, such as autonomy (Deci and Ryan, 1985; Padayachee, 2012), perceived responsibility (LaRose *et al.*, 2008; Padayachee, 2012) and self-efficacy (Padayachee, 2012; Workmen *et al.*, 2008), are considered to test employees' ISSP compliance, as shown in the proposed research model illustrated in Figure 2.

3. Research model and hypotheses

Figure 2 illustrates the proposed research model.

Autonomy is the extent to which individuals can regulate how and when they perform particular job tasks (Hackman and Oldham, 1980). Previous studies found that autonomy

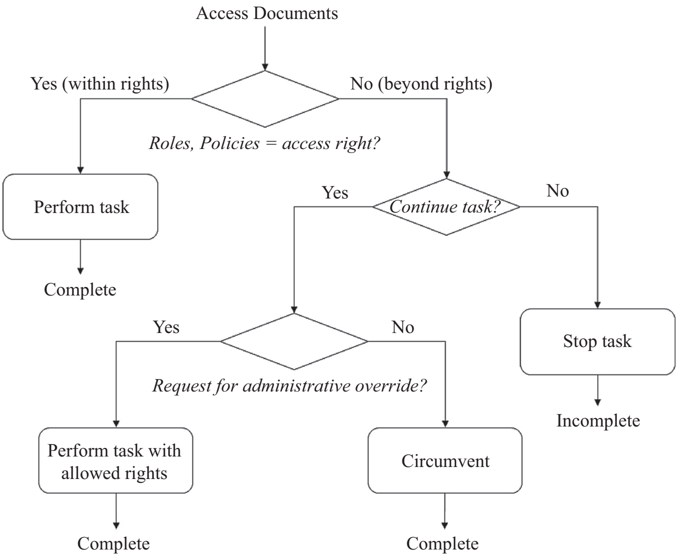


Figure 1.
EDRM system workflow (adopted from Jeon *et al.*, 2018)

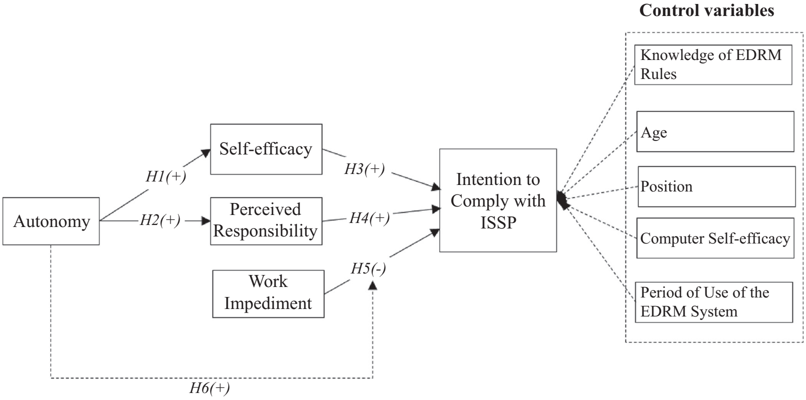


Figure 2.
Research model

could promote employee's competence and capability to address an assigned task (Parker, 1998; Sousa *et al.*, 2012). Furthermore, individuals' self-efficacy is influenced by the perception of the autonomy with which they carry out specified tasks without supervisory control (Wang and Netemyer, 2002). In the context of information security, Wall *et al.* (2013) found that intrinsic motivations such as autonomy promote consistent task-related behavior, influencing the mastery of a task and the subsequent task-specific self-efficacy. In this study, self-efficacy is defined as individuals' abilities and capabilities to use an EDRM system. In the EDRM setting, organizations restrict employees' access to information assets. However, when autonomy is permitted in an EDRM system, employees can regulate their performance and workflow regarding security-related tasks, as they can complete their assigned task without encumbrances (Jeon *et al.*, 2018). Thus, we posit that EDRM users with higher autonomy are more likely to increase their abilities and capabilities to perform security-related tasks.

H1. Autonomy exerts a positive effect on self-efficacy.

According to the job characteristic theory, as autonomy increases, employees feel a greater responsibility for the outcomes of their task because they believe their work outcome is a consequence of their own decisions and efforts (Hackman and Oldham, 1980). Furthermore, the overall level of perceived responsibility is initiated by autonomy because autonomy contributes to an employee's feelings of responsibility for the task at hand (Kiggundu, 1981). Under an EDRM system, employees may regard using the EDRM system as a responsibility overload because employees may have to accept additional responsibilities to access the EDRM system (Ahuja *et al.*, 2007). Thus, this study defines perceived responsibility as an employee's added sense of responsibility toward the consequences regarding the use of an EDRM system to access information assets (Jeon *et al.*, 2018). Based on previous studies, autonomy could be positively related to perceived responsibility (Hornung and Rousseau, 2007). In the EDRM setting, if employees can determine how and when they perform certain tasks according to EDRM workflows, employees will feel responsible for outcomes and goals beyond their individual tasks (Jeon *et al.*, 2018). Thus, our study posits that EDRM users with autonomy in performing a security-related task will feel responsibility for the outcomes of a task.

H2. Autonomy exerts a positive effect on perceived responsibility.

In the context of security policy compliance, individuals' self-efficacy affects appropriate behavioral intentions (Bulgurcu *et al.*, 2010; Herath and Rao, 2009; Johnston and Warkentin, 2010). The effect of self-efficacy on compliance intention can be explained by the protection motivation theory (Rippetoe and Rogers, 1987; Rogers, 1975). This theory posits that self-efficacy is the capability to carry out a recommended behavior and plays a role as a factor in the coping-appraisal process (Rogers, 1975). According to this theory, adaptive behavior is enhanced by the expectation that individuals can successfully execute the recommended adaptive behaviors (Rogers, 1975). Furthermore, previous studies have demonstrated that self-efficacy exerts a strong influence on an individual's attitude or information security compliance behaviors (Anderson and Agarwal, 2010; Johnston and Warkentin, 2010; Yoon and Kim, 2013). Accordingly, our study posits that an individual with self-efficacy for performing a security-related task is more likely to intend to comply with ISSP.

H3. Self-efficacy exerts a positive effect on the intention to comply with ISSP.

Individuals tend to protect themselves from, and prevent, undesirable consequences by assigned responsibility (Bandura, 2001; Schwartz, 1977; Shillair *et al.*, 2015). In this regard, responsibility promotes security-related behavior such as the use of a firewall, update of virus protection and use of a pop-up blocker (LaRose *et al.*, 2008). This implies that responsibility facilitates individuals to behave appropriately according to organizational guidelines. In the context of an EDRM system, if employees misbehave (e.g. circumvent/bypass ISSP or share passwords), they could impair their reputation or be punished. Employees who perceive a high level of responsibility are more likely to behave appropriately, as they are likely to circumvent undesirable outcomes based on rationalized conditions. Hence, our study posits that employees' perceived responsibility promotes the intention to comply with ISSP.

H4. Perceived responsibility exerts a positive effect on the intention to comply with ISSP.

Work impediment refers to the employee's sense of hindrance and interference in the performance of security-related tasks. Redundant system workflow and constraints result in work impediments. Therefore, employees tend to bypass or violate security policies when expeditiously addressing a specified task (Alter, 2014; West, 2008). That is, if redundant workflows or constraints are interfering with task completion, employees are more likely to violate the security policy. ISSP is a regulated procedure that describes the manner in which a security-related task is to be performed, which must be approved by an administrator. For example, when employees access a security system to print restricted documents, the documents must be approved. The system workflow for performing a security-related task in an urgent situation could be cumbersome and increase the time to complete the assigned task. This disincentive is likely to cause employees to follow an inappropriate workflow, such as sharing an ID and password to complete certain tasks (Vogelsmeier *et al.*, 2008). Thus, employees are likely to consider circumventing the ISSP.

H5. Work impediment exerts a negative effect on the intention to comply with ISSP.

As mentioned earlier, employees with an impediment to perform a task tend to bypass the ISSP (West, 2008). The procedures for gaining access rights to certain documents are likely to facilitate the regulation and protection of information assets in organizations. Employees, as EDRM users, cannot complete assigned tasks without authorization. In this situation, complicated procedures for receiving approval are likely to reduce employees' intention to comply with the procedure because they perceive the approval procedures as work impediments. However, Jeon *et al.* (2018) found that EDRM users with high flexibility showed higher compliance intention and lower work impediment than users with low flexibility. Thus, we posit that autonomy moderates the relationship between work impediment and ISSP compliance intention.

H6. Autonomy attenuates the negative effect of work impediment on the intention to comply with ISSP.

4. Methodology

4.1 Instrument development

To develop this study's survey instrument, measures were borrowed mainly from previous research, and a new scale for perceived responsibility was developed upon the theoretical definitions of the constructs. All constructs in the model were measured with multiple items, and each item was measured by using a seven-point Likert scale (from strongly disagree (= 1) to strongly agree (= 7)). The measure "intention to comply with ISSP" was adopted from Bulgurcu *et al.* (2010) and Herath and Rao (2009). The autonomy measure consisted of three items and was adapted from Spreitzer (1995). As part of this study, items from previous literature (Bulgurcu *et al.*, 2010) were adapted to measure work impediment based on performance of security-related tasks. Finally, to measure self-efficacy, four items adapted from Anderson and Agarwal (2010) were used in this study. The questionnaire is presented in Table 1.

This study pursues to investigate the impact of intrinsic motivation perceptions on ISSP compliance intention beyond the known predictors. Thus, the study considers five factors (i.e. knowledge of the EDRM rules, age, position, computer self-efficacy and period of use of an EDRM system). Previous studies showed that ISSP compliance intention can be influenced by age, status and computer self-efficacy (e.g. Hovav and D'Arcy, 2012; Kim and Kim, 2017). Moreover, the longer individuals use a certain IS, the more likely they are to understand the system rules and follow system policies. Thus, in this study, the period of use of an EDRM system and knowledge of EDRM rules were controlled.

4.2 Sample and data collection

To test this study's hypotheses, employees of organizations presently using Fasoo's EDRM systems were contacted. As an EDRM system production company, Fasoo has

Construct	Item	Statement	Reference
Intention to comply with ISSP (INT)	INT1	I intend to comply with the requirements of the ISSP	Bulgurcu *et al.* (2010) Herath and Rao (2009)
	INT2	I intend to protect information assets according to the requirements of the ISSP	
	INT3	I intend to carry out my responsibilities prescribed in the ISSP	
	INT4	I am likely to follow the ISSP	
	INT5	I am certain that I will follow the ISSP	
Work impediment (IMP)	IMP1	Performing task through the EDRM system ___ slows me back	Bulgurcu *et al.* (2010)
	IMP2	___ reduces my response time to my colleagues/ managers/clients	
	IMP3	___ reduces my efficiency at work	
	IMP4	___ reduces my productivity at work	
Perceived responsibility (PR)	PR1	Performing tasks through the EDRM system I consider that I have been provided excessive responsibility	*Self-developed*
	PR2	I need to reduce certain parts of my responsibilities	
	PR3	I perceive a high degree of responsibility	
	PR4	Working with external entities requires excessive responsibility	
Autonomy (AUT)	AUT1	Deploying the EDRM system provides me a chance to use my personal initiative and judgment in carrying out tasks	Spreitzer (1995)
	AUT2	I have significant autonomy in task performance through the EDRM system	
	AUT3	Performing tasks through the EDRM system provides me a considerable opportunity for independence and freedom in the manner in which I complete my task	
Self-efficacy (SEF)	SEF1	I feel comfortable about performing tasks through the EDRM system	Anderson and Agarwal (2010)
	SEF2	Performing task through the EDRM system is entirely under my control	
	SEF3	Performing task through the EDRM system is convenient	

Table 1.
Measurement instrument

provided solutions for more than 1,300 companies globally [4]. Our criterion for choosing the sample was that companies had employed an EDRM system for over three years. This is because if the period of EDRM usage was short, respondents may not possess sufficient knowledge about the EDRM system, which could result in biases in the survey results. Finally, respondents from six companies within the manufacturing industry, five companies from financial services, two government institutes, eleven companies from the information technology (IT) industry and four companies from other industries agreed to participate. Overall, the sample comprised of 28 companies and 360 participants. The valid responses, after filtering out incomplete responses, amounted to 346. Among the respondents, 62 belonged to manufacturing firms, 73 were from financial services firms, 136 belonged to IT firms, 31 were from government institutes and seven belonged to other firms. Detailed descriptive statistics related to the demographic characteristics of the respondents are summarized in Table 2.

Characteristics		Frequency	
Gender	Male	235	68%
	Female	111	32%
Age	19–25	10	3%
	26–35	191	55%
	36–45	128	37%
	46 and above	17	5%
Education	High-school diploma	3	1%
	Associate's degree	36	10%
	Bachelor degree	271	79%
	Master's degree	36	10%
Industry	Manufacturing	62	18%
	Financial services	73	21%
	IT	136	41%
	Government	31	9%
	Public institution	32	9%
	Other	7	2%
Position	Staff	88	25%
	Assistant manager	111	32%
	Manager	90	26%
	Deputy general manager	30	9%
	General manager and over	27	8%

Table 2. Demographic characteristics of respondents

5. Data analysis and results

5.1 Instrument validation

First, an exploratory factor analysis was conducted for all the measures, using principal component analysis with varimax rotation. The eigenvalues of five factors were observed to be larger than 1.0. These five factors accounted for 78.5 percent of the total variance.

To test our research model, partial least squares structural equation modeling (PLS-SEM) was used. PLS-SEM does not assume normal data distribution (Chin, 1995; Peng and Lai, 2012). The method is effective for conducting exploratory research and testing complex models with moderating effects (Pavlou and Fygenson, 2006). To ensure convergent validity and reliability, the individual items should satisfy three criteria (Chin, 1998; Fornell and Larcker, 1981). First, all the item loading values should be larger than 0.7. Second, the composite reliability should be larger than 0.8. Third, the average variance extracted (AVE) should be larger than 0.5, or the square root of the AVE should be larger than 0.7. Based on these criteria, each test result achieved a satisfactory level of convergent validity. As illustrated in Table 3, all measurement item loadings were above the recommended value of 0.7. Furthermore, the composite reliabilities of all constructs were above 0.8, and the square root of the AVE was larger than 0.7 for each construct. To achieve discriminant validity, the AVE of a construct should be larger than its correlations with all other constructs (Fornell and Larcker, 1981). Table 4 indicates that the square root of the AVE for each construct was larger than the cross-factors between the AVE and all other constructs. Thus, this study satisfied the criteria for discriminant validity.

5.2 Structural model test

After establishing the validity of the survey instrument, each hypothesis was tested using WarpPLS, which provides several measures in the form of model fit and quality indices (Kock, 2015). For satisfactory predictive and explanatory quality, the *p*-values of the average path coefficient, average R^2 and average adjusted R^2 should be below 0.05 (Rosenthal and

Table 3.
Item loadings and cross-loadings

	1	2	3	4	5
INT1	*0.86*	−0.16	0.06	−0.24	−0.19
INT2	*0.89*	−0.02	0.07	0.01	−0.04
INT3	*0.93*	0.09	0.02	0.00	0.02
INT4	*0.91*	0.02	−0.01	0.01	0.06
INT5	*0.76*	0.01	−0.22	0.25	0.15
IMP1	0.00	*0.88*	−0.03	−0.02	−0.07
IMP2	0.02	*0.91*	−0.08	−0.01	0.05
IMP3	−0.01	*0.87*	0.08	−0.01	0.00
IMP4	−0.02	*0.88*	0.03	0.04	0.02
PR1	0.08	−0.05	*0.83*	0.04	−0.09
PR2	−0.02	−0.03	*0.89*	−0.02	0.07
PR3	−0.04	−0.09	*0.89*	−0.07	−0.11
PR4	−0.02	0.17	*0.87*	0.05	0.13
AUT1	−0.08	−0.07	0.07	*0.76*	0.05
AUT2	0.06	0.00	−0.03	*0.74*	−0.05
AUT3	0.00	0.05	−0.03	*0.77*	0.00
SEF1	−0.05	−0.01	0.11	−0.01	*0.73*
SEF2	−0.02	0.02	−0.07	0.00	*0.74*
SEF3	0.07	−0.01	−0.04	0.01	*0.71*

Note(s): Legend: 1 = intention to comply with ISSP, 2 = work impediment, 3 = perceived responsibility, 4 = autonomy, 5 = self-efficacy. The italic numbers in Table 3 indicates that the loading values of corresponding measures of each variable is higher than those of other measures

Table 4.
Composite reliability, AVE and latent variable correlations

	1	2	3	4	5
Intention to comply with ISSP	*0.819*				
Work impediment	−0.171	*0.926*			
Perceived responsibility	0.038	0.400	*0.884*		
Autonomy	0.151	−0.188	0.192	*0.923*	
Self-efficacy	0.282	−0.176	0.012	0.349	*0.934*
Composite reliability	0.909	0.960	0.934	0.945	0.953
Cronbach's α	0.871	0.944	0.906	0.913	0.926
AVEs	0.670	0.857	0.781	0.853	0.872

Note(s): Square roots of average variances extracted (AVEs) listed on diagonal

Rosnow, 1991), and the value of the average block variance inflation factor and average full collinearity variance inflation factor should be below 3.3 (Kock and Lynn, 2012). Tenenhaus' goodness of fit (GoF) measures a model's explanatory power (Tenenhaus *et al.*, 2005). GoF is *small* if equal to or greater than 0.1, *medium* if equal to or greater than 0.25 and *large* if equal to or greater than 0.36 (Wetzels *et al.*, 2009). The values of all measures satisfied these criteria and did not cause any critical problems in the structural model.

As presented in Table 5, the proposed model exhibits adequate predictive and explanatory power.

The structural model results are presented in Figure 3. As hypothesized earlier in this study, all path coefficients were significant. Autonomy significantly influenced self-efficacy and responsibility ($\beta = 0.35, p < 0.001; \beta = 0.19, p < 0.001$). The results indicate that H1 and H2 were supported. Self-efficacy exerted a significant effect on ISSP compliance intention ($\beta = 0.21; p < 0.001$). The intention to comply with ISSP was predicted using responsibility ($\beta = 0.09; p < 0.05$) and work impediment ($\beta = -0.15; p < 0.01$). Therefore, H3, H4 and H5 were also supported. Finally, a moderating analysis was conducted, as suggested by Kock (2014). The two subgroups were split by the mean value of autonomy ($M = 3.84$). The result shows that an employee's autonomy exerted significant influence as a moderator of the relationship between work impediment and compliance intention ($\beta = 0.1$; $p < 0.05$), indicating that H6 was supported. As shown in Figure 4, the results suggest that employees with high levels of work impediments will have a stronger intention to comply with ISSP under high autonomy as compared to under low autonomy.

6. Discussion

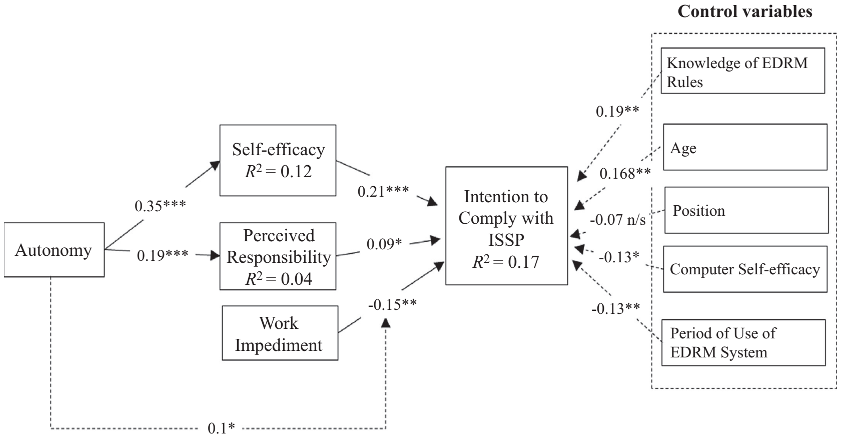
6.1 Research observations

This study was conducted in the context of an EDRM system based on field survey data regarding employees' intrinsic motivations to adhere to information security rules. This study extends the information security literature by demonstrating that the intrinsic motivations of employees increase ISSP compliance intentions. The study also determines that autonomy can mitigate the negative effect of work impediment on ISSP compliance intentions.

This study produced several significant observations. First, although previous research has shown inconsistent results, this study indicates that self-efficacy in a security-related task exerts a positive influence on the intention to comply with ISSP. That means that an

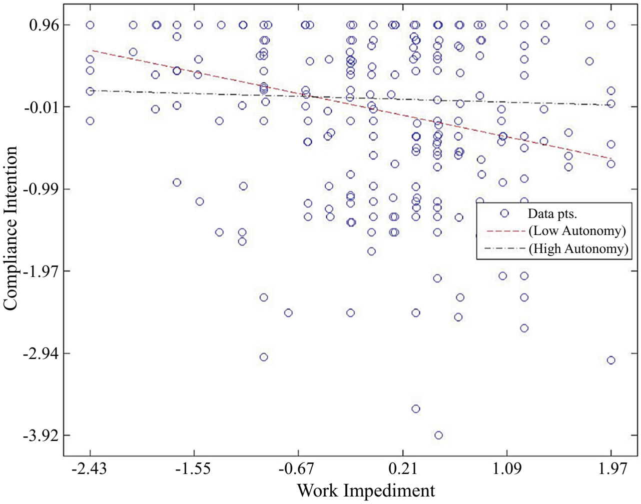
Measure	Value	Criteria
Average path coefficient	0.162 ($p < 0.001$)	Acceptable if $p < 0.05$
Average R^2	0.108 ($p = 0.001$)	
Average adjusted R^2	0.099 ($p = 0.003$)	
Average block VIF	1.494	Acceptable if ≤ 3.3
Average full collinearity VIF	1.501	Acceptable if ≤ 3.3
Tenenhaus GoF	0.312	Small if ≥ 0.1 Medium if ≥ 0.25 Large if ≥ 0.36

Table 5. Structural model fit and quality indices



Note(s): Path significance: *$p < 0.05$,**$p < 0.01$,***$p < 0.001$; n/s = not significant

Figure 3. SEM-PLS results



Graph with low-high values of moderating variables and data points (standardized scales)

Figure 4.
Moderating effect of autonomy on the relationship between work impediment and intention to comply with ISSP

employee's capability and confidence to perform a security-related task results in an appropriate behavioral outcome, namely, compliance with ISSP.

Second, perceived responsibility in the outcome of a security-related task exerts a positive effect on the intention to comply with ISSP. Employees assume certain responsibilities when they perform a security-related task. Thus, employees handle a security-related task with caution because its outcome is entirely a result of their decisions. That is, perceived responsibility in performing a security-related task can motivate employees to comply with ISSP. Thus, it is crucial for employees to perceive their responsibilities when performing security-related tasks.

Third, work impediment exerts a negative effect on the intention to comply with ISSP. Under perceived constraints, employees tend to violate the system workflow (i.e. security policy/regulation) because the completion of a task through the required procedures requires more time and effort (Kobayashi *et al.*, 2005; Lawton, 1998; Siponen and Vance, 2010; West, 2008). Accordingly, work impediment may result in sharing password and ID to reduce the effort and time consumed. It constitutes a potential information security threat involving unauthorized disclosure. Thus, the employee's negative perception regarding compliance with ISSP should be reduced. In this regard, our study demonstrates the moderating effect of autonomy on the relationship between work impediment and ISSP compliance intention. Considering the importance of mitigating the negative effect of work impediment on ISSP compliance intention, this moderation is critical.

Four, this study demonstrates the significant positive effect of autonomy on self-efficacy. The observation is consistent with that of the study by Wall *et al.* (2013), which demonstrated the significant role of intrinsic motivation (i.e. autonomy) in generating self-efficacy. This study highlights the significant role of autonomy in generating self-efficacy in the information security context. That is, perceived freedom and discretion in security-related tasks affect an employee's capability to perform their tasks.

Finally, this study observes the positive relationship between autonomy and responsibility. To the best of present authors' knowledge, such an observation has not been reported in previous IS security research. Similar to the significant role of autonomy in generating self-efficacy (Langfred and Moye, 2004; Zhou, 1998) in a general work setting, this study demonstrates the significant role that autonomy plays in generating perceived responsibility (e.g. discretion and freedom in security-related tasks yield perceived responsibility) in the IS security context.

6.2 Implications

This study leads to several implications and contributions to theory. The primary contribution of the study is its examination of how employees' intrinsic motivations facilitate compliance with ISSP. In this regard, this study provides a deeper understanding of the effect of autonomy as an intrinsic motivation for ISSP compliance.

In the information security literature, end users' perceptions toward a data-centric security system (i.e. EDRM system) and antecedents of EDRM rule compliance have not been addressed. Therefore, this study enhances information security literature by identifying the psychological factors affecting ISSP compliance (i.e. autonomy, perceived responsibility and self-efficacy) using the intrinsic motivation perspective.

Few studies focus on autonomy-related information security compliance, and most involve initial and explorative stages of research (e.g. Pham *et al.*, 2016). To the best of our knowledge, this study is one of the first to statistically examine the effects of autonomy by using a specific security system case, EDRM. The results indicate that freedom and discretion in a security-related task exert a significant influence on perceived responsibility and self-efficacy.

Practitioners should note that autonomy can influence compliance with ISSP. The results of this study indicate measures for increasing an employee's intention of compliance with ISSP. This study has implications for the induction of compliance behavior. As an information security system, the EDRM system is a conventional security method that enforces compliance with ISSP through access control. For promoting compliance with ISSP, this study offers a concept wherein an organization should be aware of its employees' perceptions of responsibility and self-efficacy as well as of their autonomy.

Organizations can set policies involving autonomy that increase appropriate behavioral outcomes through security-related task responsibility and self-efficacy. Furthermore, it is observed that work impediment results in noncompliance behavior. Organizations can attempt to reduce inappropriate procedural tasks by enhancing autonomy rather than by over-regulating security-related tasks. Effective and efficient information security measures should be implemented, and technical support related to information security issues should be responsive and helpful to the users.

Additionally, observations indicate that organizations should aim to increase perceived responsibility and to enhance the capability to perform security-related tasks. To increase perceived responsibility and self-efficacy, organizations could provide security education training and awareness programs. Thus, employees perceive their responsibility for the outcome of a security-related task, and the capability to perform such tasks could be increased.

Finally, the demands for ISSP compliance could be perceived as a work impediment. Although the concept of ISSP has been established by adapting several international standards and best practices, employees' negative perceptions could result in unforeseen outcomes. In this situation, the results of this study indicate that granting autonomy in performing security-related tasks helps to mitigate the negative effect of work impediment on ISSP compliance.

7. Conclusion

Information security in the workplace is an essential part of IS operations that protects organizational knowledge and business assets to ensure market competence. Organizations have employed diverse ways to encourage their employees to comply with organizational information security policies. Prior studies on information security have investigated the means of motivating workers to follow organizational rules and regulations on information security. However, limited studies have focused on the effect of intrinsic motivation, in encouraging employees and enabling their ISSP compliance. The primary purpose of this study is to examine the effect of intrinsic motivations on information security compliance. This study provides important new insights on the voluntary compliance of security system users. Although our study's findings constitute meaningful implications in terms of intrinsic motivations and information security compliance in organizations, there are limitations in terms of the research settings. First, the analyzed data were collected from companies in South Korea that have employed specific EDRM systems. This means that EDRM system users could differently evaluate other types of EDRM systems because the user interface is different for different companies that have developed the EDRM system. Therefore, a greater variety of EDRM systems should be included in future research, thereby increasing generalizability. Second, the current study explores the positive role of intrinsic motivation in enhancing ISSP compliance. In our research, autonomy is a primary construct to empirically investigate such encouraging roles, and this study applies a self-determination perspective to propose a theoretical background of autonomy. Owing to our research focus, the current study does not cover all major aspects of the self-determination theory, such as autonomy, competency and relatedness, which are suggested in previous literature. Further study is required to elaborate the proposed research model such that the ISSP compliance exploration includes extended aspects of the self-determination theory. Third, this study focuses specifically on EDRM rule compliance intention. Future research could extend to other types of security systems to improve the model's external validity. Lastly, this study examined employees' perception toward information security systems. Based on this study, future research could compare information security users between autonomy-embedded security systems and conventional security systems. Such comparison can evaluate the robustness of the effect of autonomy.

Notes

1. http://www.isdecisions.com/insider-threat-persona-study/.
2. The peripheral security method is a method for protecting information assets against external attack. It relies on the security of a network and its applications, such as firewalls, intrusion detection systems and virtual private networks.
3. In this study, it is assumed that security-related tasks are implemented through an EDRM system. Hence, the term "performing security-related tasks" is used interchangeably with the term "access to the EDRM system."
4. https://en.fasoo.com/?lang=en.

References

Ahuja, M.K., Chudoba, K.M., Kacmar, C.J., McKnight, D.H. and George, J.F. (2007), "IT road warriors: balancing work-family conflict, job autonomy, and work overload to mitigate turnover intentions", *MIS Quarterly,* Vol. 33 No. 1, pp. 1-17.

Alter, S. (2014), "Theory of workarounds", *Communications of the Association for Information Systems*, Vol. 34, pp. 1041-1066.

Anderson, C.L. and Agarwal, R. (2010), "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions", *MIS Quarterly,* Vol. 34 No. 3, pp. 613-643.

Ayyagari, R. (2012), "An exploratory analysis of data breaches from 2005-2011: trends and insights", *Journal of Information Privacy and Security,* Vol. 8 No. 2, pp. 33-56.

Bandura, A. (2001), "Social cognitive theory: an agentic perspective", *Annual Review of Psychology*, Vol. 52 No. 1, pp. 1-26.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirial study of rationality-based beliefs and information security awareness", *MIS Quartely*, Vol. 34 No. 3, pp. 523-548.

Chin, W.W. (1995), "Partial least squares is to lisrel as principal components analysis is to common factor analysis", *Technology Studies,* Vol. 2, pp. 315-319.

Chin, W.W. (1998), "The partial least squares approach to structural equation modeling", *Modern Methods for Business Research*, Vol. 295 No. 2, pp. 295-336.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers and Security*, Vol. 32, pp. 90-101.

D'Arcy, J., Hovav, A. and Galleta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No 1, pp. 79-98.

Deci, E.L. and Ryan, R.M. (1985), "The general causality orientations scale: self-determination in personality", *Journal of Research in Personality*, Vol. 19 No. 2, pp. 109-134.

Deci, E.L. and Ryan, R.M. (1987), "The support of autonomy and the control of behavior", *Journal of Personality and Social Psychology*, Vol. 53 No. 6, pp. 1024-1037.

Deci, E.L., Eghrari, H., Patrick, B.C. and Leone, D.R. (1994), "Facilitating internalization: the self-determination theory perspective", *Journal of Personality*, Vol. 62 No. 1, pp. 119-142.

Dhillon, G. (2007), *Principles of Information Systems Security: Text and Cases*, John Wiley and Sons, Hoboken, NJ.

Ferneley, E.H. and Sobreperez, P. (2006), "Resist, comply or workaround? An examination of different facets of user engagement with information systems", *European Journal of Information Systems*, Vol. 15 No. 4, pp. 345-356.

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 3, pp. 39-50.

Hackman, J.R. and Oldham, G.R. (1980), *Work Redesign*, Addison Wesley, Reading, MA.

Hennessy, S., Lauer, G., Zunic, N., Gerber, B. and Nelson, A. (2009), "Data-centric security: integrating data privacy and data security", *IBM Journal of Research and Development*, Vol. 53 No. 2, pp. 1-12.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125.

Hornung, S. and Rousseau, D.M. (2007), "Active on the job—proactive in change: how autonomy at work contributes to employee support for organizational change", *The Journal of Applied Behavioral Science*, Vol. 43 No. 2, pp. 401-426.

Hovav, A. and D'Arcy, J. (2012), "Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US and South Korea", *Information and Management*, Vol. 49 No. 2, pp. 99-110.

Hovav, A. and Putri, F.F. (2016), "This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy", *Pervasive and Mobile Computing*, Vol. 32, pp. 35-49.

Jeon, S.H., Hovav, A., Han, J.Y. and Alter, S. (2018), "Rethinking the prevailing security paradigm: can user empowerment with traceabiltiy reduce the rate of security policy circumvention?", *The DATABASE for Advances in Information Systems*, Vol. 49 No. 3, pp. 54-77.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly*, Vol. 34 No. 3, pp. 549-566.

Ke, W. and Zhang, P. (2010), "The effect of extrinsic motivation and satisfaction in open source software development", *Journal of the Association for Information Systems*, Vol. 11 No. 12, pp. 784-808.

Ke, W., Tan, C.-H., Sia, C.-L. and Wei, K.K. (2012), "Inducing Intrinsic motivation to explore the enterprise system: the supermacy organizational levers", *Journal of Management Information Systems*, Vol. 23 No. 3, pp. 257-289.

Kiggundu, M.N. (1981), "Task interdependence and the theory of job design", *Academy of Management Review*, Vol. 6 No. 3, pp. 499-508.

Kim, S.S. and Kim, Y.J. (2017), "The effect of compliance knowledge and compliance support systems on information security compliance behavior", *Journal of Knowledge Management*, Vol. 21 No. 4, pp. 986-1010.

Kobayashi, M., Fussell, S.R., Xiao, Y. and Seagull, F.J. (2005), "Work coordination, workflow, and workarounds in a medical context", *Paper presented at the CHI'05 Extended Abstracts on Human Factors in Computing Systems*, 2 April -7 April, Portalnd, USA, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.93.7967&rep=rep1&type=pdf (accessed January 2018).

Kock, N. and Lynn, G. (2012), "Lateral collinearity and misleading results in variance-based SEM: an illustration and recommendations", *Journal of the Association for Information Systems*, Vol. 13 No. 7, pp. 1-40.

Kock, N. (2014), "Using data labels to discover moderating effects in PLS-based structural equation modeling", *International Journal of E-Collaboration*, Vol. 10 No. 4, pp. 1-14.

Kock, N. (2015), "WarpPLS 5.0 user manual", available at: http://cits.tamiu.edu/WarpPLS/UserManual_v_5_0.pdf/ (accessed March 2018).

Langfred, C.W. and Moye, N.A. (2004), "Effects of task autonomy on performance: an extended model considering motivational, informational, and structural mechanisms", *Journal of Applied Psychology*, Vol. 89 No. 6, pp. 934-945.

LaRose, R., Rifon, N.J. and Enbody, R. (2008), "Promoting personal responsibility for internet safety", *Communications of the ACM*, Vol. 51 No. 3, pp. 71-76.

Lawton, R. (1998), "Not working to rule: understanding procedural violations at work", *Safety Science*, Vol. 28 No. 2, pp. 77-95.

Liang, H., Xue, Y. and Wu, L. (2013), "Ensuring employees' IT compliance: carrot or stick?", *Information Systems Research*, Vol. 24 No. 2, pp. 279-294.

Morin, J.H. and Hovav, A. (2012), "Strategic value and drivers behind organizational adoption of enterprise DRM: the Korean case", *Journal of Service Science Research*, Vol. 4 No. 1, pp. 143-168.

Morin, J. and Pawlak, M. (2007), *From Digital Rights Management to Enterprise Rights and Policy Management: Challenges and Opportunities*, IGI Global, Hershey, PA.

Padayachee, D. (2012), "Taxonomy of compliant information security behavior", *Computer and Security*, Vol. 31 No. 5, pp. 673-680.

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' behavior towards IS security policy compliance", in *40th annual hawaii international conference on System Sciences in Hawaii*, USA, 2007, IEEE, p. 156b.

Parker, S.K. (1998), "Enhancing role breadth self-efficacy: the roles of job enrichment and other organizational interventions", *Journal of Applied Psychology*, Vol. 83 No. 6, pp. 835-852.

Pavey, L. and Sparks, P. (2009), "Reactance, autonomy, and path to persuasion: examining perceptions of threats to freedom and informational value", *Motivation and Emotion*, Vol. 33 No. 3, pp. 277-290.

Pavlou, P.A. and Fygenson, M. (2006), "Understanding and predicting electronic commerce adoption: an extension of the theory of planned behavior", *MIS Quarterly*, Vol. 30 No.1, pp. 115-143.

Peng, D.X. and Lai, F.J. (2012), "Using partial least squares in operations management research: a practical guideline and summary of past research", *Journal of Operations Management*, Vol. 30 No. 6, pp. 467-480.

Pham, H.C., El-Den, J. and Richardson, J. (2016), "Stress-based security compliance model–an exploratory study", *Information and Computer Security*, Vol. 24 No. 4, pp. 326-347.

Rippetoe, P.A. and Rogers, R.W. (1987), "Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat", *Journal of Personality and Social Psychology*, Vol. 52 No. 3, pp. 596-604.

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change1", *Journal of Psychology*, Vol. 91 No. 1, pp. 93-114.

Rosenthal, R. and Rosnow, R.L. (1991), *Essentials of Behavioral Research: Methods and Data Analysis*, Vol. 2, McGraw-Hill, New York, NY.

Ryan, R.M. and Deci, E.L. (1985), *Intrinsic Motivation and Self-Determination in Human Behavior*, Plenum Press, New York, NY.

Ryan, R.M. and Deci, E.L. (2000), "Self-determination theory and facilitation of intrinsic motivation, social development, and well-being", *American Psychologist*, Vol. 55 No. 1, pp. 68-78.

Schwartz, S.H. (1977), "Normative influences on altruism", *Advances in Experimental Social Psychology*, Vol. 10, pp. 221-279.

Shillair, R., Cotten, S.R., Tsai, H.Y.S., Alhabash, S., Larose, R. and Rifon, N.J. (2015), "Online safety begins with you and me: convincing Internet users to protect themselves", *Computers in Human Behavior*, Vol. 48, pp. 199-207.

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2014), "Employees' adherence to information security policies: an exploratory field study", *Information and Management*, Vol. 51 No. 2, pp. 217-224.

Son, J.Y. (2011), "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies", *Information and Management*, Vol. 48 No. 7, pp. 296-302.

Sousa, C.M., Coelho, F. and Guillamon-Saorin, E. (2012), "Personal values, autonomy, and self-efficacy: evidence from frontline service employees", *International Journal of Selection and Assessment*, Vol. 20 No. 2, pp. 159-170.

Spreitzer, G.M. (1995), "Psychological empowedrment in the workplace - dimensions, measurement, and validation", *Academy of Management Journal*, Vol. 38 No. 5, pp. 1442-1465.

Tenenhaus, M., Vinzi, V.E., Chatelin, Y.M. and Lauro, C. (2005), "PLS path modeling", *Computational Statistics and Data Analysis*, Vol. 48 No. 1, pp. 159-205.

Tyler, T.R. and Blader, S.L. (2005). "Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings", *Academy of Management Journal,* Vol. 48 No. 6, pp. 1143-1158.

Vogelsmeier, A.A., Halbesleben, J.R. and Scott-Cawiezell, J.R. (2008), "Technology implementation and workarounds in the nursing home", *Journal of the American Medical Informatics Association*, Vol. 15 No. 1, pp. 114-119.

Wall, J.D., Palvia, P. and Lowry, P.B. (2013), "Control-related motivations and information security policy compliance: the role of autonomy and efficacy", *Journal of Information Privacy and Security*, Vol. 9 No. 4, pp. 52-79.

Wang, G. and Netemyer, R.G. (2002), "The effects of job autonomy, customer demandingness, and trait competitiveness on salesperson learning, self-efficacy, and performance", *Journal of the Academy of Marketing Science*, Vol. 30 No. 3, pp. 217-228.

Warkentin, M. and Willison, R. (2009), "Behavioral and policy issues in information systems security: the insider threat", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 101-105.

Warkentin, M., Johnston, A.C. and Shropshire, J. (2011), "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention", *European Journal of Information Systems*, Vol. 20 No. 3, pp. 267-284.

West, R. (2008), "The psychology of security", *Communications of the ACM*, Vol. 51 No. 4, pp. 34-40.

Wetzels, M., Odekerken-Schröder, G. and Van Oppen, C. (2009), "Using PLS path modeling for assessing hierarchical construct models: guidelines and empirical illustration", *MIS Quarterly*, Vol. 33 No. 1, pp. 177-195.

Workman, M., Bommer, W.H. and Straub, D. (2008), "Security lapses and the omission of information security measures: a threat control model and empirical test", *Computers in Human Behavior*, Vol. 24 No. 2, pp. 799-816.

Yoon, C. and Kim, H. (2013), "Understanding computer security behavioral intention in the workplace: an empirical study of Korean firms", *Information Technology and People*, Vol. 26 No. 4, pp. 401-419.

Zhou, J. (1998), "Feedback valence, feedback style, task autonomy, and achievement orientation: interactive effects on creative performance", *Journal of Applied Psychology*, Vol. 83 No. 2, pp. 261-276.

Corresponding author
Jinyoung Han can be contacted at: han1618@cau.ac.kr