Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2018 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-26-2018

# Understanding the Roles of Challenge Security Demands, Psychological Resources in Information Security Policy Noncompliance

Ying Li
*Dalian University of Technology*, yingli@dlut.edu.cn

Nan Zhang
*Harbin Institute of Technology*, andyzhang@hit.edu.cn

Ting Pan
*Dalian University of Technology*, pantingdlut@foxmail.com

# Understanding the Roles of Challenge Security Demands, Psychological Resources in Information Security Policy Noncompliance

*Completed Research Paper*

**Ying Li**
Dalian University of Technology
No.2 Linggong Road, Gangjingzi District,
Dalian, Liaoning, P.R.China, 116023
yingli@dlut.edu.cn

**Nan Zhang**
Harbin Institute of Technology
No.13 Fayuan Street, Nangang District,
Harbin, Heilongjiang, P.R.China, 150001
andyzhang@hit.edu.cn

**Ting Pan**
Dalian University of Technology
No.2 Linggong Road, Gangjingzi District, Dalian, Liaoning, P.R.China, 116023
panting@mail.dlut.edu.cn

**Abstract**

*It is widely agreed that employees' noncompliance with information security policies (ISP) is still a major problem for organizations. In order to understand the factors that reduce employees' ISP noncompliance, previous studies have focused on stressful security demands that consequently aggravate noncompliance, and tangible job resources to promote compliance. However, how security demands encourage employees to comply and how intangible resources affect employees' ISP noncompliance have been largely overlooked. In this study, we posit and argue that challenge security demands and intangible psychological resources can help promote employees' ISP compliance. Drawing on the Job Demands-Resources Model and the theory of psychological resource, we specifically examine the roles of continuity demand, mandatory demand as challenge security demands, and felt trust, professional development and personal resource as psychological resources in influencing employees' ISP noncompliance. The proposed model is validated by survey data from 224 employees. The theoretical and practical contributions are also discussed.*

**Keywords:** Information security policy noncompliance, job demands-resources model, challenge security demands, psychological resources, personal resource

## Introduction

Employees' noncompliance with information security policies (ISP) has continued being a serious threat to organizations' information security. A recent report suggests that employees are the top source that causes security incidents, as 84% of security incidents are attributed to their misbehavior (PWC 2017). Similarly, in another report, 73% of the selected companies rated employee errors and omissions as top threats to organizations (Deloitte 2013). Increasing scholars and practitioners have devoted efforts to investigating the reasons for employees' ISP noncompliance and the measures to control it.

In order to regulate employees' security behavior, organizations make ISP, of which, security demands are a very important component. Numbers of studies have examined employees' perceptions

of security demands in ISP and their roles in affecting employees' ISP (non)compliance. Typically, previous studies have examined two types of security demands in employees' perceptions: "challenges" and "hindrances". Challenge security demands tend to promote compliance, whereas hindrance security demands tend to thwart compliance. For example, previous research has suggested that several perceptions of security demands increase stress and therefore are hindrances to compliance, such as work overload, complexity, uncertainty (D'Arcy et al. 2014, Hwang and Cha 2018), access to security policies, security compliance overload (Pham et al. 2016), etc. Hindrance demands usually lead to ISP violation as they increase employees' level of moral disengagement (D'Arcy et al. 2014) and decrease their organizational commitment (Hwang and Cha 2018). Other studies have investigated the perceptions of security demands as challenges that can promote compliance, such as monitoring (D'Arcy et al. 2009), mandatoriness (Boss et al. 2009), security countermeasures (Hovav and D'Arcy 2012), accountability (Vance et al. 2015), certainty of control (Chen et al. 2012), etc. Several studies understand the impact of challenge security demands on ISP (non)compliance through deterrence, suggesting that the security demands can increase employees' perception of sanction certainty, severity, and therefore decrease the noncompliance intention (e.g., D'Arcy et al. 2009, Hovav and D'Arcy 2012). However, challenge demands do not only deter employees but could also encourage employees to comply. The extant literature lacks the understanding of why and how challenge security demands drive employees' positive psychological state and then lead to ISP compliance.

In order to encourage employees to meet the security demands, organizations often provide relevant resources. Previous studies have mainly focused on resources that are tangible, such as SETA programs (D'Arcy et al. 2009), facilitating conditions (Ng and Rahim 2005, Pahnila et al. 2007), resource availability (Herath and Rao 2009), top management participation (Hu et al. 2012), rewards (Bulgurcu et al. 2010), etc. Such tangible resources are important, however, the intangible resources in terms of employees' psychological resources have been largely neglected. Psychological resources can be the social and personal resources that individuals centrally value in their own right and help achieve certain goals (Hobfoll 2002). In this regard, self-efficacy has received the most research attention in existing literature (e.g., Bulgurcu et al. 2010; Chatterjee et al. 2015). Self-efficacy represents a psychological resource that individuals see themselves having the ability to successfully influence their environment and accomplish the goals. However, psychological resources are not limited to self-efficacy but include the resources that can be obtained from organization, job, or even the individual self. In the context of information security, psychological resources such as the benefits that employees can get by performing a security task (e.g., knowledge mastered), the social support obtained by compliance (e.g., trust by others), and personal resource that an individual owns (e.g., effort) to meet the security demands may be helpful in understanding employees' ISP (non)compliance.

To summarize the above, we have identified two gaps in extant IS security behavior literature. First, previous research has not paid enough attention to the process how challenge security demands reduce ISP noncompliance. Second, existing research has not examined the roles of psychological resources as motivations in promoting ISP compliance. In order to fill in the two gaps, in this study, we attempt to explain how challenge security demands and psychological resources can help understand employees' noncompliance with ISP. Drawing from the job demands-resources model (Demerouti et al. 2001) and the theory of psychological resource (Hobfoll 2002), we specifically explore the continuity demand, mandatory demand as challenge security demands to decrease employees' intention to ISP noncompliance. We also argue that felt trust, professional development as intangible job resources are supportive factors that help employees to meet the security demands. Further, we propose that perseverance of effort as a personal resource mediates the relationships between security demands, job resources, and ISP noncompliance intention. We collect survey data to test our proposed model. The findings have implications for both theory and practice.

# Theoretical Background

## *Job Demands-Resources Model*

Job Demands-Resources (JD-R) model is a work performance model, explaining that employees' job performance can be affected by both demands and resources of job characteristics (Bakker et al. 2007; Xanthopoulou et al. 2008). Job demands refer to "those physical, social, or organizational aspects of the job that require sustained physical or mental effort, and therefore, are associated with certain physiological and psychological costs" (Demerouti et al. 2001. p. 501). Crawford et al. (2010) have differentiated two categories of job demands: hindrances and challenges. The hindrance process explains that job demands may increase the stress and lead to a job strain (Bakker and Demerouti 2007; Tremblay and Messervey 2011). When faced with excessive demands, employees resort to compensatory strategies in order to maintain an adequate level of job performance, which wears out employees' energy and then subsequently leads them to adopt a cynical attitude towards their work. Information security scholars have found similar findings, suggesting that stressful security requirements increase the possibility of ISP violation (D'Arcy et al. 2014; Hwang and Cha 2018). However, scholars in psychology argue that when people appraise the job demands as challenges that have the potential to promote personal growth or gains, people tend to perform an active or problem-solving style of coping. In other words, individuals may be more willing to invest themselves in response to challenging demands because they view meeting demands as meaningful and desirable (Kahn 1990; Lazarus and Folkman 1984). Previous information security research has only addressed the hindrance process but overlooked the challenge process that may motivate employees' ISP compliance.

JD-R model suggests another motivational process by adding job resources. Job resources are defined as "those physical, social, or organizational aspects of the job that may do any of the following: (a) be functional in achieving work goals; (b) reduce job demands and the associated physiological and psychological costs; (c) stimulate personal growth and development" (Demerouti et al. 2001, p. 501). Examples of job resources are feedback, job control, and social support (Schaufeli et al. 2004). A lack of resources may lead to reduced motivation and disengagement, therefore, lead to withdrawal behavior. In information security behavior literature, scholars have explored a lot of job resources that help achieve ISP compliance. For example, security education, training, and awareness program is typical job resource to promote employees' security awareness and behavior (D'Arcy et al. 2009). In another example, facilitating conditions in terms of easy access to security policies, manual IT assistance can help employees remove obstacles at work and promote compliance (Herath and Rao 2009, Pahnila et al. 2007). One common feature of such resources is they are tangible. In contrast, Bakker et al. (2007) suggested that intangible job resources also affect employees' behavior, for example, he argued that supervisor support is a type of intangible job resources and is positively related to work engagement. Similarly, Xanthopoulou et al. (2009) found that autonomy, coaching, and team climate is a typical intangible job resource related to work engagement and financial returns. However, the intangible job resources have been largely overlooked in ISP (non)compliance research.

## *Psychological Resource*

Psychological resource refers to non-cognitive psychological elements that originate from within individuals but emerge collectively as shaped by the organization to become a source of competitive advantage (Li and Champion 2015). Psychological resources enhance health, well-being, and resistance to stress (Taylor et al 2000). Psychological resource theories suggest that higher levels of psychological resources are favorable, especially in highly challenging circumstances, are related to more active goal-directed behavior and better psychological outcomes (Carver and Scheier 1999; Hobfoll 1998). People with psychological resources are able to better cope with the demands of a situation and are more capable of solving problems in stressful circumstances. They may interpret situations as less stressful than people with fewer resources (Hobfoll 2002). Psychological resources can be in various forms, such as in the form of conditions (e.g., self-respect, social support, job control), personal characteristics (e.g., efficacy, beliefs), and energies (e.g., opportunities for skill development) (Hobfoll 2001).

Personal resource is a psychological resource that refers to an employee's belief of their ability to control internal resources such as energy, time and effort, which impact upon the environment successfully (Hobfoll et al. 2003). The internal belief is a thought, explanation, and evaluation of the external situation (Tremblay and Messervey 2011). Grover et al. (2017) suggested that personal resource is directly and negatively related to work stress because of buffering the relation of external demands on psychological stress. And previous researchers have found the direct effect of personal resource on work engagement (Shahpouri et al 2016; Xanthopoulou et al 2009). In addition, Hobfoll (2002) has suggested that social support is a key psychological resource from the social environment, which can refer to the perceptions of receipt of support, and aspects of the self and whether it is viewed as supported. Individuals who have social support are more stress resistant. In information security behavior literature, Burns et al. (2017) have proposed a similar concept called psychological capital. The authors view psychological capital as a type of psychological resource that includes the personality-based resources such as optimism, self-efficacy and resilience, and the motivational state such as hope. The authors found that psychological capital influences insiders' threat appraisal and coping appraisal in organizations.

## Research Model and Hypotheses

Based on the JD-R model and the theory of psychological resources, we propose an integrated research model to explain employees' noncompliance with ISP, see Figure 1. In the proposed model, we explain the impacts of challenge security demands, intangible job resources and personal resource on ISP noncompliance intention. Challenge security demands is a second-order construct that is formatively composed of continuity demand and mandatory demand. Intangible job resources are a second-order construct that is formatively composed of felt trust and professional development. For personal resource, we examine a specific construct named perseverance of effort.

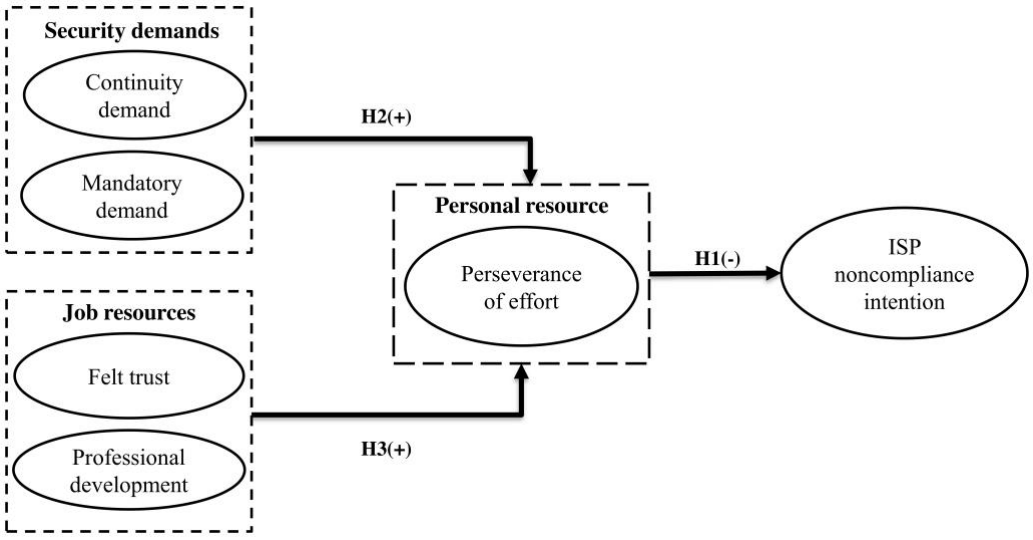


**Figure 1. Research model**

### *Perseverance of Effort*

In this study, we examine perseverance of effort as a personal resource in our research model, because employees' information security behavior usually requires more effort than other types of personal resources, such as time and energy. In line with the definition of personal resource, perseverance of effort in this study refers to an employee's belief of the ability to control and affect the environment by devoting his/her efforts. Perseverance of effort plays an essential role in shaping employee's behavior when faced with obstacles and it also leads to higher attainment (Mooradian et al. 2016). Researchers found that employees with high perseverance of effort appear to have more flexible performing ways and coping strategies with greater persistence (Staw et al. 1994). Employees may be

more committed and engaged in their jobs because they derive fulfillment from it (Kirkman and Shapiro 2001). In the IS literature, people with a high level of perceived control can increase perseverance of effort that strengthens the intention to perform the behavior (Ajzen 2002). Similarly, the research found that employee in high perseverance spent more effort in complying with IS security policies in difficult scenarios, such as locking a computer on the desk at the company (Johnston et al. 2016). In line with the existing literature, we propose that an employee's level of perseverance of effort will decrease their ISP noncompliance intention.

*H1: Perseverance of effort is negatively related to employees' ISP noncompliance intention.*

## *Challenge Security Demands*

In this study, challenge security demands describe the situations that security demands or requirements provide employees opportunities to learn, achieve, and demonstrate the type of competence that tends to get rewarded (Crawford et al. 2010). We examine employees' perceptions of two challenge security demands: continuity demand and mandatory demand. Continuity demand refers to the security demand that one should align his/her behavior with the security policies consistently, without exception. Continuity emphasizes the present and future through repetition (such as making the same choice at "all times" or "every time") to convey the ongoingness and repetitiveness of actions (Brigham et al. 2014). Hershfield et al. (2012) found that people who hold continuity beliefs are more likely to make ethical decisions. In our context, employees who perceive continuity demand is aware that their continuous compliance is valuable and expected by the organizations (Vedadi 2016). Mandatory demand refers to the security demand that compliance with existing security policies and procedures is compulsory or expected by organizational management (Boss et al. 2009). In principle, employees should always behave according to the ISP. However, sometimes, employees need to make trade-offs, such as security vs. convenience, in which cases, conforming to the security demands are challenging. In such situations, successfully addressing security concerns and solving security problems may show one's competence in work. In information security context, Lowry and Moody (2015) suggested that when employees perceive organizational security policy as mandatory, they are more likely to persevere in taking precautions. For both continuity and mandatory demand, employees may feel that meeting the challenge demands is meaningful and desirable (Kahn 1990; Lazarus and Folkman 1984). Hobfoll (1998) and Baltes (1997) suggest that successfully addressing challenging circumstances will result in increased resources. In the similar vein, we hypothesize that employees who perceive the challenge security demands may be motivated to put more efforts to meet the demands. Therefore, we hypothesize that,

*H2: An employee's perception of challenge security demands is positively associated with his/her perseverance of effort.*

## *Intangible Job Resources*

We propose two intangible job resources in this study, namely, felt trust and professional development. Felt trust refers to the perception and realization of others' positive expectations and exposes their willingness to be vulnerable (Lau et al. 2014). In an organizational context, felt trust represents a social support that one can obtain from relevant others, such as managers and co-workers. Trustees are often willing to accept such positive information, which increases their confidence in their own ability an importance, increasing their motivation to complete difficult tasks (Lau et al. 2014). If employees have a sense of felt trustworthiness from their coworkers, they will exhibit better work attitudes and performance (Lester and Brower 2003). From a social exchange perspective (Blau 1964), when a person is trusted, in exchange, he or she feels somewhat obligated to fulfill the hope of the trustors, and exert effort to meet their expectations. Previous is a type of social support that motivates individuals to perform the expected behavior in information security situations (Johnston et al. 2010). It reflects the opinions of significant others (such as the immediate supervisors and co-workers), who may formally or informally evaluate an employees' performance. Managers' or co-workers' trust may be one of the employees' motivations to comply with ISP (Hsu et al. 2015; Johnston et al. 2010). In this sense, felt trust is an intangible job resource to encourage employees to

invest more personal resource to meet the security demands. If employees have a sense of felt trustworthiness from their coworkers, they will exhibit better work attitudes and performance (Lester and Brower 2003).

Professional development is a type of intangible job resource that can promote or maintain professional competence, such as acquire professional knowledge and master professional skills (Bakker et al. 2003). Karasek and Theorell (1990) have argued that jobs conductive learning opportunities may result in employees being intrinsically involved in their jobs. As professional development is expected in jobs with requirements for skill enhancement, decision-making, and responsibility (Dunckel 2002), opportunities to learn are deemed important for employees. Professional development may be an important resource for employees to cope with the continuous updating of knowledge and skills that legal profession requires, reduce uncertainty and enhance well-being at work (Panari et al. 2010). In the context of ISP compliance, when employees face with challenge security situations, such as the conflict of security and convenience, employees may be motivated to put effort to overcome the difficulties or solve the security problems in work, because finding solutions is an opportunity for learning and improving their professionalism. Therefore, we hypothesize that,

*H3: An employee's perception of intangible job resources is positively associated with his/her perseverance of effort.*

## Methodology

### *Measurement Development*

We used a scenario-based survey method to test our proposed model. In order to make realistic and believable scenarios, we designed the scenarios together with the security managers from the company where we collected the data. First, the security managers listed the IS security problems that concerned them, covering a wide range of issues such as the secure use of mobile devices, secure emailing, secure behavior when traveling, and secure use of the Internet. Based on their list, we composed specific scenarios. The security managers then evaluated whether or not these scenarios were relevant to their situations, and they helped edit them. After two rounds of modifications, we finalized four scenarios that were regarded as the most relevant to the company: a. Unauthorized portable devices for storing corporate data, b. Sending unencrypted emails, c. Not locking a computer on the desk at the company, d. Downloading suspicious files from the Internet. All items were adapted from previous studies to fit the current context. Seven-point Likert scales were used anchored from 1 (strongly disagree) to 7 (strongly agree). The specific scenarios and items are shown in Appendix A.

We conducted a pilot study before the primary data collection. Since the wordings were just slightly different among the three scenarios, we used one scenario (unauthorized portable devices for storing corporate data) to pilot the survey. We invited our faculty members, Ph.D. students, and any researchers familiar with the topic to complete the survey and provide comments on our questions. The pilot sample size was 39. We assessed reliability by using Cronbach's α, and the convergent and discriminant validity by using principal components analysis. The assessment indicated acceptable results for the instrument.

### *Data Collection*

We conducted the primary data collection at a global insurance company. We randomly send the online survey to 893 employees. Each respondent was randomly assigned to one of the four scenarios and corresponding questions. We received 224 responses, with a response rate of 25%. In the final sample, 51% of the respondents were male, 76% were in the 26-55 age range.

## Data Analysis and Results

We used SmartPLS v2.0 to analyze our research model. We chose the partial least square-based structural equation modeling (PLS-SEM) technique because security demands and job resources in

our model are multidimensional second-order formatively constructs, for which PLS-SEM methods are better suited.

### *Measurement Model*

For the reflective constructs, we assessed internal consistency and convergent validity by examining item loading, Cronbach's α, composite reliability, and average variance extracted (AVE) (Gefen and Straub 2005). We compared the results (see Table 1) with the commonly accepted guidelines. For reliability, the composite reliability of the constructs was greater than 0.8, and Cronbach's α was greater than 0.7 (Chin 1998). For convergent validity, indicator loadings exceeded 0.7 (Chin 1998), and AVE for each reflective construct exceeded 0.5. We performed a bootstrap with 1,000 resamples and examined the t-values of the outer model loadings. All the indicators exhibited loadings that were significant ($p < 0.001$), denoting strong convergent validity.

For the discriminant validity, all items loaded higher on their respective constructs than on the other constructs, and the cross-loading differences were much higher than the suggested threshold of 0.1 (Gefen and Straub 2005). The square root of the AVE of each construct was higher than the inter-construct correlations (Fornell and Larcker 1981, see Table 2). The correlations among all constructs were all well below the 0.90 thresholds, suggesting that all constructs were distinct from each other (Herath and Rao 2009).

**Table 1. Descriptive Statistics**

| Construct | Sub-construct | Mean | SD | Alpha | CR | AVE |
|---|---|---|---|---|---|---|
| Noncompliance intention (INT) | N/A | 2.55 | 1.87 | 0.85 | 0.93 | 0.87 |
| Perseverance of effort (PE) | N/A | 5.91 | 1.12 | 0.89 | 0.93 | 0.81 |
| Challenge job demands (JD) | Continuity demand (CON) | 5.85 | 1.18 | 0.87 | 0.92 | 0.80 |
| | Mandatory demand (MAN) | 6.08 | 1.08 | 0.91 | 0.96 | 0.92 |
| Intangible job resources (JR) | Felt trust (FT) | 5.15 | 1.52 | 0.91 | 0.96 | 0.92 |
| | Professional development (PD) | 5.08 | 1.58 | 0.87 | 0.92 | 0.80 |

Note: SD= standard deviation, Alpha= Cronbach's α, CR= composite reliability, AVE= Average variance extracted.

**Table 2. Latent Variable Correlations and the Square Root of AVE**

| Construct | INT | PE | CON | MAN | FT | PD |
|---|---|---|---|---|---|---|
| INT | **0.93** | | | | | |
| PE | -0.49 | **0.90** | | | | |
| CON | -0.48 | 0.66 | **0.89** | | | |
| MAN | -0.53 | 0.70 | 0.82 | **0.96** | | |
| FT | -0.40 | 0.61 | 0.53 | 0.59 | **0.96** | |
| PD | -0.18 | 0.27 | 0.32 | 0.34 | 0.34 | **0.89** |

Note: Bold items are the square root of the AVE.

In our model, security demands and job resources are second-order formatively constructs. They are a reflective-formative type of hierarchical component models. Security demands are formatively constructed by two reflective first-order constructs: continuity demand and mandatory demand. Job resources are formatively constructed by two reflective first-order constructs: felt trust and professional development. We followed the two-stage approach suggested by Ringle et al. (2012) to test the hierarchical component model. First, we used the repeated indicators approach to obtain the

latent variable score for the lower order components. Second, we used the latent variable scores as the formative indicators of the second-order construct. Our validation results suggest that all reflective measures demonstrated satisfactory reliability and construct validity and that the formative measures demonstrated satisfactory construct. Therefore, all of the measures were valid and reliable.

### *Structural Model*

Our results of the full model were consistent with our theory, as shown in Figure 2. Perseverance of effort had a significant negative effect ($\beta = -0.46$, $p < 0.001$) on noncompliance intention, which supports H1. Job demands had a significant positive effect ($\beta = 0.61$, $p < 0.001$) on perseverance of effort, which supports H2. Job resources had a significant positive effect ($\beta = 0.18$, $p < 0.05$) on perseverance of effort, which supports H3.

Perseverance of effort explained 26% of the variance in noncompliance intention. Job demands and job resources collectively explained 52% of the variance in perseverance of effort. Three control factors (age, IT knowledge and computer experience) were insignificant. Gender was significant ($\beta = -0.14$, $p < 0.001$), which indicated that males are more likely to violate ISP. In summary, the results provide support for all of the hypotheses we proposed. Detailed results are provided in Figure 2.

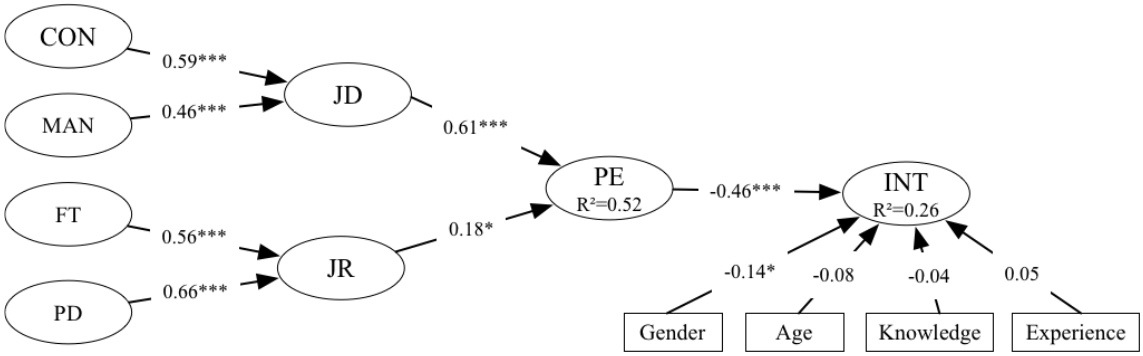


**Figure 2. Structural Model Results**

## Discussion

The main purpose of this study is to explain employees' ISP noncompliance from the combined perspectives of challenge security demands and psychological resources. We examined the roles of continuity demand, mandatory demand, felt trust, professional development, and perseverance of effort in decreasing employees' ISP noncompliance intention. Our empirical results have supported all our hypotheses.

Our study makes three theoretical contributions to the literature of ISP (non)compliance. First, our study is one of the pioneering studies to explain ISP noncompliance from the perspective of demands and resources. Drawing on the framework of job demands and resources model and the theory of psychological resource, we figured out the specific security demands and psychological resources that influence employees' noncompliance intention with ISP. Compared with the traditional JD-R models, we got different findings. Previous studies in organizational context found that job demands decrease employees' job performance (Crawford et al. 2010) and security compliance behaviors (Pham et al. 2016). In our study, we managed to show that when employees perceive security demands as challenge, they are willing to invest more effort and less likely to violate ISP.

Second, we enriched the JD-R model in ISP (non)compliance context by defining different types of demands and resources. In terms of the demands, previous security studies view security demands as stress, which thwart compliance. In our study, we define security demands as challenge, which could promote ISP compliance. In addition, a large number of security studies examined the tangible resources in work and organization. By contrast, our study focused more on the intangible job

resources, such as felt trust and professional development. Our work extends the understanding of job demands and resources in a security context.

Third, we extended the JD-R model by adding a different type of resource –personal resource. In our study, personal resource plays an intermediate role in the relationship between security demands, job resources and the ISP noncompliance. Both challenge security demands and intangible job resources increase the level of personal resource, which in turn decreases ISP noncompliance. In doing so, we managed to explain the process that how challenge security demands together with job resources influence employees' noncompliance.

Our study has practical implications for the management of employees' security behavior in organizations. Our study suggests that when organizations make information security demands and requirements, the demands should be within employees' appropriate level of confidence and competence in their ability to meet them. The demands should neither be too strict nor too stressful. Employees have the motivations to meet the demands if they are challenging rather than stressful. For example, organizations can address that following the ISP at any time is an important way to ensure security. Make clear security demands and design training to let employees understand that following the policies are imperative. In addition, organizations should create the trust atmosphere and culture that employees' efforts are highly respected. Employees should be highly encouraged to actively learn security skills and knowledge to overcome the difficulties or solve security problems independently. By doing so, employees' information security behavior can be better regulated.

## Conclusion

Many organizations are putting efforts in regulating employees' information security behavior, including making appropriate information security policies and provide necessary resources to ensure employees' compliance. In order to figure out what kind of security demands are effective and what resources organizations should provide to employees, we conduct this study. Drawing on JD-R model and the theory of psychological resources, we proposed that challenge security demands, such as continuity demand and mandatory demand can decrease employees' ISP noncompliance. We also proposed that psychological resources such as perseverance of effort, felt trust and professional development are important in encouraging employees' ISP compliance. Our empirical data has supported our hypotheses. Our study extends the existing understanding of ISP compliance. Furthermore, our study suggests organizations to make challenging rather than stressful security policies, and create trust and opportunities to learn for employees to increase their effort to comply.

## Acknowledgments

This research was supported by the Ministry of Education of Humanities and Social Science project (17YJC630072), China Postdoctoral Science Foundation (2016M601315), Doctoral Scientific Research Foundation of Liaoning Province (20170520435), and National Natural Science Foundation of China (71431002, 71421001, 71272092).

## References

Ajzen, I. 2002. "Perceived Behavioral Control, Self-efficacy, Locus of Control, and the Theory of Planned Behavior," *Journal of Applied Social Psychology* (32:4), pp. 665-683.

Bakker, A. B., and Demerouti, E. 2007. "The Job Demands-Resources Model: State of the Art," *Journal of Managerial Psychology* (22:3), pp. 309-328.

Bakker, A. B., Demerouti, E., Taris, T. W., Schaufeli, W. B., and Schreurs, P. J. G. 2003. "A Multigroup Analysis of the Job Demands-Resources Model in Four Home Care Organizations," *International Journal of Stress Management* (10:1), pp. 16-38.

Bakker, A. B., Hakanen, J. J., Demerouti, E., and Xanthopoulou, D. 2007. "Job Resources Boost Work Engagement, Particularly When Job Demands are High," *Journal of Educational Psychology* (99:2), pp. 274-285.

Baltes, P. B. 1997. "On the Incomplete Architecture of Human Ontogeny: Selection, Optimization, and Compensation as Foundation of Developmental Theory," *American Psychologist* (52:4), pp. 366-380.

Blau, P. M. 1964. *Exchange and Power in Social Life*, John Wiley, New York.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.

Brigham, K. H., Lumpkin, G. T., Payne, G. T., and Zachary, M. A. 2014. "Researching Long-Term Orientation: A Validation Study and Recommendations for Future Research," *Family Business Review* (27:1), pp. 72-88.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Burns, A. J., Posey, C., Roberts, T. L., and Lowry, P. B. 2017. "Examining the Relationship of Organizational Insiders' Psychological Capital with Information Security Threat and Coping Appraisals," *Computers in Human Behavior* (68:1), pp. 190-209.

Carver, C. S., and Scheier, M. F. 1999. "Stress, Coping, and Self-Regulatory Processes," In *Handbook of personality: Theory and research*, L. A. Pervin and O. P. John (eds.), New York: Guilford Press, pp. 553-575.

Chatterjee, S., Sarker, S., and Valacich, J. S. 2015. "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use," *Journal of Management Information Systems* (31:4), pp. 49-87.

Chen, Y., Ramamurthy, K., and Wen, K. W. 2012. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *Journal of Management Information Systems* (29:3), pp. 157-188.

Chin, W.W. 1998. "Issues and Opinion on Structural Equation Modeling," *MIS Quarterly* (22:1), pp. Vii–Xvi.

Crawford, E. R., LePine, J. A., and Rich, B. L. 2010. "Linking Job Demands and Resources to Employee Engagement and Burnout: A Theoretical Extension and Meta-Analytic Test," *Journal of Applied Psychology* (95:5), pp. 834-848.

D'Arcy, J., Herath, T., and Shoss, M.K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285–318.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Deloitte 2013. Blurring the Lines: 2013 TMT Global Security Study. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/dttl_TMT_GlobalSecurityStudy_English_final_020113.pdf. Assessed 2015/4/23

Demerouti, E., Bakker, A. B., Nachreiner, F., and Schaufeli, W. B. 2001. "The Job Demands-Resources Model of Burnout," *Journal of Applied psychology* (86:3), pp. 499-512.

Dunckel, H. 2002. "Job Analysis and Work Roles," in *International Encyclopedia of the Social and Behavioral Sciences*, N. J. Smelser and P. B. Baltes (eds.), London: Elsevier, pp. 7973-7977.

Gefen, D., and Straub, D.W. 2005. "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example," *Communications of the Association for Information Systems* (16:1), pp. 91-109.

Grover, S. L., Teo, S. T., Pick, D., and Roche, M. 2017. "Mindfulness as A Personal Resource to Reduce Work Stress in the Job Demands-Resources Model," *Stress and Health* (33:4), pp. 426-436.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations," *European Journal of Information Systems* (18:2), pp. 106-125.

Hershfield, H.E., Cohen, T.R. and Thompson, L. 2012. "Short Horizons and Tempting Situations: Lack of Continuity to Our Future Selves Leads to Unethical Decision Making and Behavior," *Organizational Behavior and Human Decision Processes* (117:2), pp. 298–310.

Hobfoll, S. E. 1998. *Stress, Culture, and Community: The Psychology and Philosophy of Stress*, New York: Plenum.

Hobfoll, S. E. 2001. "The Influence of Culture, Community, and the Nested-Self in the Stress Process: Advancing Conservation of Resources Theory," *Applied Psychology* (50:3), pp. 337-421.

Hobfoll, S. E. 2002. "Social and Psychological Resources and Adaptation," *Review of General Psychology* (6:4), pp. 307-324.

Hobfoll, S. E., Johnson, R. J., Ennis, N., and Jackson, A. P. 2003. "Resource Loss, Resource Gain, and Emotional Outcomes among Inner City Women," *Journal of Personality and Social Psychology* (84:3), pp. 632-643.

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* (49:2), pp. 99-110.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., and Lowry, P. B. 2015. "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness," *Information Systems Research* (26:2), pp. 282-300.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Sciences* (43:4), pp. 615-660.

Hwang, I., and Cha, O. 2018. "Examining Technostress Creators and Role Stress as Potential Threats to Employees' Information Security Compliance," *Computers in Human Behavior* (81), pp. 282-293.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:1), pp. 1-20.

Johnston, A. C., Warkentin, M., McBride, M., and Carter, L. 2016. "Dispositional and Situational Factors: Influences on Information Security Policy Violations," *European Journal of Information Systems* (25:3), pp. 231-251.

Kahn, W. A. 1990. "Psychological Conditions of Personal Engagement and Disengagement at Work," *Academy of Management Journal* (33:4), pp. 692-724.

Karasek, R.A. and Theorell, T. 1990. *Healthy Work: Stress, Productivity, and the Reconstruction of Working Life*, New York, NY: Basic Books.

Kim, T. Y., Wang, J., and Chen, J. 2016. "Mutual Trust Between Leader and Subordinate and Employee Outcomes," *Journal of Business Ethics* (133:4), pp. 619-632.

Kirkman, B. L., and Shapiro, D. L. 2001. "The Impact of Cultural Values on Job Satisfaction and Organizational Commitment in Self-Managing Work Teams: The Mediating Role of Employee Resistance," *Academy of Management Journal* (44:3), pp. 557-569.

Lau, D. C., Lam, L. W., and Wen, S. S. 2014. "Examining the Effects of Feeling Trusted by Supervisors in the Workplace: A Self-Evaluative Perspective," *Journal of Organizational Behavior* (35:2), pp. 112–127.

Lazarus, R. S., and Folkman, S. 1984. "Coping and Adaptation," in *The handbook of behavioral medicine*, G. V. Coelho, D. A. Hamburg, and J. E. Adams (eds.), New York: Basic Books, pp. 282-325.

Lester, S. W., and Brower, H. H. 2003. "In the Eyes of the Beholder: The Relationship Between Subordinates' Felt Trustworthiness and Their Work Attitudes and Behaviors," *Journal of Leadership and Organizational Studies* (10:2), pp. 17-33.

Li P, and Campion M C. 2015. "How Psychological Resources Contribute to Sustainable Competitive Advantage," *Academy of Management Annual Meeting Proceedings* (2015:1), pp. 18539-18549.

Lowry, P. B., and Moody, G. D. 2015. "Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organizational Information Security Policies," *Information Systems Journal* (25:5), pp. 433-463.

Mooradian, T., Matzler, K., Uzelac, B., and Bauer, F. 2016. "Perspiration and Inspiration: Grit and Innovativeness as Antecedents of Entrepreneurial Success," *Journal of Economic Psychology* (56:1), pp. 232-243.

Moss, T.W., Payne, G.T., and Moore, C.B. 2014. "Strategic Consistency of Exploration and Exploitation in Family Businesses," *Family Business Review* (27:1), 51–71.

Ng, B. Y., and Rahim, M. 2005. "A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security," in *Proceedings of the 9th Pacific Asia Conference on Information System*, Bangkok, Thailand, pp. 234-247.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior towards IS Security Policy Compliance," in *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, Washington, DC, pp. 156-166.

Panari, C., Guglielmi, D., Simbula, S., and Depolo, M. 2010. "Can an Opportunity to Learn at Work Reduce Stress? A Revisitation of the Job Demand-Control Model," *Journal of Workplace Learning* (22:3), pp. 166-179.

Pham, H. C., El-Den, J., and Richardson, J. 2016. "Stress-Based Security Compliance Model–An Exploratory Study," *Information and Computer Security* (24:4), pp. 326-347.

PWC. 2017. "The Global State of Information Security Survey: Strengthening Digital Society against Cyber Shocks," https://www.pwc.com/us/en/cybersecurity/information-security-survey/strengthening-digital-society-against-cyber-shocks.html Assessed 2017/12/23

Ringle, C.M., Sarstedt, M. and Straub, D.W. 2012. "A Critical Look at the Use of PLS-SEM in MIS Quarterly," *MIS Quarterly* (36:1), pp. 3-14.

Schaufeli, W. B., and Bakker, A. B. 2004. "Job Demands, Job Resources, and Their Relationship with Burnout and Engagement: A Multi-Sample Study," *Journal of Organizational Behavior* (25:3), pp. 293-315.

Shahpouri, S., Namdari, K., and Abedi, A. 2016. "Mediating Role of work Engagement in the Relationship Between Job Resources and Personal Resources with Turnover Intention Among Female Nurses," *Applied Nursing Research* (30:1), pp. 216-221.

Staw, B. M., Sutton, R. I., and Pelled, L. H. 1994. "Employee Positive Emotion and Favorable Outcomes at the Workplace," *Organization Science* (5:1), pp. 51-71.

Taylor, S. E., Kemeny, M. E., Geoffrey, M. R., Bower, J. E., and Gruenewald, T. L. 2000. "Psychological Resources, Positive Illusions, and Health," *American Psychologist* (55:1), pp. 99-109.

Tremblay, M. A., and Messervey, D. 2011. "The Job Demands-Resources Model: Further Evidence for the Buffering Effect of Personal Resources," *SA Journal of Industrial Psychology* (37:2), pp. 10-19.

Vance, A. O., Lowry, P. B., and Eggett, D. 2015. "Increasing Accountability Through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations," *MIS Quarterly* (39:2), PP. 345-366.

Vedadi, A. 2016. "Continuous Secure Behavior from Process Memory Model Perspective," *Twenty-second Americas Conference on Information Systems*.

Xanthopoulou, D., Bakker, A. B., Heuven, E., Demerouti, E., and Schaufeli, W. B. 2008. "Working in the Sky: A Diary Study on Work Engagement among Flight Attendants," *Journal of Occupational Health Psychology* (13:4), pp. 345-356.

# Appendix

## *Scenarios*

In the scenarios, we describe a situation that Newman, an employee of your company, is facing. Please read the scenario carefully first, and then indicate the extent to which you agree with the following statements.

*Scenario 1: Unauthorized portable devices for storing corporate data*

Newman wants to copy a file and show it to clients at their meeting. A personal unencrypted USB stick is available nearby. The file contains the contract draft. However, the meeting is starting soon, and it takes time to find an encrypted USB stick. Newman decides to copy the file into the personal unencrypted USB stick.

*Scenario 2: Sending unencrypted emails*

Newman needs to send an encrypted email to a client. The client says that she has difficulties decrypting the email and asks Newman to send her an unencrypted one. The file contains the contract draft. However, the client says that, if she cannot open the email, she may consider switching to another company. So, Newman decides to send an unencrypted email to her.

*Scenario 3: Not locking a computer on the desk at the company*

Newman has a busy morning that is filled with meetings with supervisors and colleagues. Newman must leave the desk and return several times. Newman has a long password and it is annoying that it must be used to lock and unlock the computer every few minutes. Therefore, Newman decides not to lock the computer.

*Scenario 4: Downloading suspicious files from the Internet*

Newman needs to search for some information from the Internet in order to complete some work. A file on a website is thought to contain the required information, but Newman is unsure that the site is trustworthy. The browser also displays a security warning stating that "this file type can potentially harm your computer." However, it takes time to find the information by other means, and the file helps to complete the work more quickly. Newman decides to download it.

### *Measurement Items*

| | |
|---|---|
| ISP Noncompliance intention (Adapted from Vance et al. 2012) | An example measure is as follows.<br>INT1 If you were Newman, what is the likelihood that you would have copied the file into a personal unencrypted USB stick?<br>INT2 I could see myself copying the file into a personal unencrypted USB stick if I were in Newman's situation. |
| Perseverance of effort (Adapted from Duckworth et al. 2007) | PE1 I do not mind extra work if it could ensure my organization's information security.<br>PE2 I do not mind sacrificing my immediate benefit if it could ensure my organization's information security.<br>PE3 I do not mind putting forth additional effort if it could ensure my organization's information security. |
| Continuity demand (Adapted from Brigham et al. 2014) | CON1 It is vital that I avoid the behavior every time I face this situation.<br>CON2 It is valuable for me to always avoid the behavior without exception.<br>CON3 As long as I am at work, avoiding the behavior has value. |
| Mandatory demand (Adapted from Boss et al. 2009) | MAN1 For the sake of my organization's information security, it is necessary to avoid the behavior.<br>MAN2 For eliminating the threats to my organization's information, it is imperative to avoid the behavior. |
| Felt trust (Adapted from Kim et al. 2016) | FT1 If my colleagues knew that I avoided the behavior, they might recognize me as a trustworthy co-worker.<br>FT2 If my colleagues knew that I avoided the behavior, they might recognize me as a responsible co-worker. |
| Professional development (Adapted from Bakker et al. 2003) | PD1 Finding alternative ways for me to securely do the work is an opportunity for me to master more information protection skills.<br>PD2 It is an opportunity for me to acquire more information security knowledge if I find alternative secure ways to do the work.<br>PD3 If I find alternative secure ways to do the work, I have an opportunity to use a wide range of abilities. |