The Influence of Information Security Stress on Security Policy Compliance: A Protection Motivation Theory Perspective

Shih-Hsien Chang  
Ingrasys Technology Inc., cubiccute@gmail.com

Hui-Mei Hsu  
National Kaohsiung Normal University, hmhsu@nknu.edu.tw

Yuzhu Li  
University of Massachusetts -Dartmouth, yli3@umassd.edu

Jack Shih-Chieh Hsu  
National Sun Yat-sen University, jackshsu@mis.nsysu.edu.tw

Follow this and additional works at: https://aisel.aisnet.org/pacis2018

Recommended Citation
https://aisel.aisnet.org/pacis2018/250

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2018 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
The Influence of Information Security Stress on Security Policy Compliance: A Protection Motivation Theory Perspective

Abstract

The occurrence of security incidents will not only cause substantial loss to the enterprise but also serious damage to goodwill. An enterprise has to formulate and implement effective security policies to reduce the occurrence of security incidents. However, the process of promoting the security policy will put stress on employees. The focus of this paper is whether these pressures will affect staff's compliance with the security policies based on the protection motivation theory. This study uses a survey method and 324 responses are collected. The results show that security task stress and security job stress have a significant impact on the formation of security role stress. Security role stress impacts threat and coping appraisals leading to security compliance.

Keywords: Protection motivation theory, Information security compliance, Security job stress, Security role stress, Security task stress

Introduction

As the rapid growth of new technologies, information flow in an enterprise becomes complex and diverse, which makes securing and protecting information a big challenge. Internet-based enterprise systems makes isolation no longer exist and elevates system vulnerability. Information security management expands from PCs and servers inside a company to cloud platforms. The prevalence of industrial ecosystems further extends the scope of information security management to include other vendors. The damage to enterprises caused by information security breaches could be devastating (Dlamini et al. 2009). According to a report, the number of total identities exposed has reached 429 million in 2015 (Symantec 2016). Such a huge amount of loss keeps reminding us of the importance of information security management. External information security threats evolve from virus and worm.
of early years to DDoS attack and ransomware nowadays. However, internal threat is the greatest among all the threats (Im and Baskerville 2005). The PwC report showed that 36% of information security breaches were conducted by internal members (PwC 2015). The rising internal threats attract a significant amount of attention on enterprise information auditing.

Organizations carefully develop information security policies and spend considerable effort to promote the security policies and make full disclosure, education and communication to organizational members. However, there are many factors that affect the willingness of employees to comply with the security policy. Studies have shown that the stress placed on employees by the organization's information security requirements may affect employee willingness to comply with security policies and may even further violate security policies (D’Arcy et al. 2014). However, how stress affect employees’ willingness is not explained. In addition to security-related stress, are there any other factors affecting employees’ willingness to comply with the security policy? This study aims to answer these two research questions.

**Literature Reviews**

**Information Security Compliance**

New threats that are not addressed by existing security goals constantly appear, creating a major problem for defining information security around security objectives (Cherdantseva and Hiltonb 2015). Information security was initially discussed at the technical level. Schneier (2009) points out the importance of the management level to information security and describes information security as a series of processes to understand threats, security policy development and countermeasures to address threats. Lacey (2009) proves the importance of science and technology for information security, and stresses that human factor plays an essential role on information security. Recent literature has pointed out that users with system login privileges may harm the information systems by mistake, carelessness, or deliberate compromise. Since the impact of insider events on insiders is significant, some earlier studies focus on preventing the misuse of information. Willison (2006) argues that the incidence of internal security events can be reduced by system controls to reduce the possibility of information abuse by insiders. Lee et al. (2004) suggest that strengthening organizational factors to promote social bonds is an effective way to reduce information misuse. Straub and Nance (1990) argue that companies should impose penalties on insiders for causing significant information security breaches to discourage other members of the organization from creating similar security problems.

Although early research focuses on control, penalty, and social norms, etc. to reduce potential threats of insiders to information security these mechanisms may not be sufficient for employees to comply with security policies (Stanton et al. 2005). Consequently many follow-up studies attempt to find out key elements to motivate employees to comply with security policies. Pahnila et al. (2007) propose a theoretical model that information quality and facilitating conditions have a significant impact on information security compliance. Herath and Rao (2009) argue that the willingness of employees to comply with security policies depends on the processes of threat appraisal and coping appraisal according to the protection motivation theory. Facing a security threat, employees go through a serious of cognitive process to evaluate the threat, and then decide the response and approach to cope with the threat. In this study, we will also use the protection motivation theory to explore its relationship with the information security compliance.

**Protection Motivation Theory**

The protection motivation theory (PMT) of was first proposed by (Rogers 1975; Rogers 1983) to explain threat appraisals and a series of cognitive processes when an individual faces a health threat. The architecture of protection motivational theory is mainly composed of two parts, one is the threat appraisal, and the other is coping appraisal. Threat appraisal includes threat vulnerability, threat severity and rewards. Coping appraisal is composited by 3 elements, response efficacy, self-efficacy, and response costs. Protection motivation drives behavior change (Rogers 1983). After this cognitive process, a person may adopt adaptive or maladaptive responses (Rogers 1983). Adaptive responses...
refer to actions that reduce threats, while maladaptive responses are actions that reduce the fear of threats, but do not actually help reduce or minimize threats.

The PMT was applied to study health-related behaviors initially. Researchers have proposed to use the PMT as a framework for studying information security compliance (Herath and Rao 2009, Ifinedo 2012), information assets protection (Posey et al. 2011; Posey et al. 2015), network security (Lee et al. 2008), and the enhancement of password protection (Jenkins et al. 2014). Although many studies have used the PMT to explain information security compliance, the antecedents of threat and coping appraisal are discussed insufficiently. As a result, this study attempts to extend the PMT to find out the mechanism that will affect a person’s threat appraisal and coping appraisal, eventually leading to the varied extent of information security compliance.

**Security related Stress**

Brod (1984) first defined the term technostress, which he argues is: "a modern disease of adaptation caused by an inability to cope with the new computer technologies in a healthy manner". Indeed, modern workers are often called upon to work overtime and simultaneously. As a result, there is not enough time and energy to learn new computer technologies. When things go beyond the scope of what employees can handle, stress comes into existence (Richard and Folkman 1984). The stressors of technostress are broadly divided into five categories, techno-complexity, insecurity, invasion, overload and uncertainty (Tarafdar et al. 2007). When new technologies are complex, employees must spend a lot of time and effort to learn new technologies. Many employees feel insecure because they are afraid that their jobs are being replaced by others who know better about new technologies. At the same time, the convenience of technologies makes employees easy to be contacted, creating an overlap of work time and personal time. Employees may feel overloaded because they have to use less time to complete more work with the new technological support. The fast-evolving technology makes it difficult for employees to specialize in a system and to acquire new skills in short intervals (Tarafdar et al. 2007).

Recently, technostress has been extended by researchers to study security-related stress. Security-related stress is resulted from information security requirements. D’Arcy et al. (2014) explore the relationship between security-related stress and intentional violation of security policy through the perspective of moral disengagement theory. They examined security-related stress by three different views as security-related overload, security-related complexity, and security-related uncertainty. The results of the study found that the requirements of information security increase the staff’s moral disengagement and ultimately lead to violation of security policies. Lee et al. (2016) explore security-related stress from a person-environment fit theory and transaction-based perspective. The results show that overload and privacy invasion have a significant impact on information security compliance. These two studies transfer the construct of technostress to information security, but non-technological stress is not focused.

Ament and Haag (2016) argues that non-technological security-related stress also plays an important role in compliance with security policy. Employees’ work, personal and social environment should be considered when security-related stress is studied. Following Ament & Haag (2016) this study adopts the technological and non-technological security-related stress and explore its impact on threat and coping appraisals based on protection motivation theory and information security compliance.

**Research Model and Hypotheses Development**

Based on the protection motivation theory and the literature review of security-related stress and information security compliance, we propose the research model in Figure 1. Security-related stress includes three dimensions, security job stress, security task stress, and security role stress (Ament and Haag 2016). Security task stress refers to security related stress from work environment including complexity, overload, and uncertainty (Ament and Haag 2016). Security job stress refers to security related stress from personal environment including privacy invasion, job insecurity, and degree of freedom (Ament and Haag 2016). Security role stress refers to security related stress from social environment including role conflict, self-role distance, and role ambiguity (Ament and Haag 2016, Fernandes and Tewari 2012, Vanishree 2014). Based on the protection motivation theory, the cognitive
process is divided into two appraisals, respectively coping appraisal and threat appraisal. The variables evaluated in the threat appraisal are vulnerability and severity, while the variables evaluated in the coping appraisal are response efficacy and self-efficacy. The final dependent variable is security compliance.

Figure 1. Proposed Research Model

Security role stress refers to personal feelings of dysfunction resulting from perceived security requirements in the environments and personal reactions to the requirements (Hwang and Cha 2018). When employees perform their tasks, the complexity, overload, and uncertainty of security technology from work environment brings security task stress to employees. Employees find out conflicts between their normal functional roles and security roles when it is hard to fulfill security requirements and functional duties at the same time. Tarafdar et al. (2007) shows that technostress has an influence on the productivity of staff through role stress since employees’ roles change because of organizational adoption of new technologies. The security related stresses from personal environment including job insecurity, privacy invasion, and degree of freedom make employees hard to separate personal and work time and prioritize the goals and requirements. Therefore, we hypothesize that

Hypothesis 1. Security job stress will positively increase security role stress.

Hypothesis 2. Security task stress will positively increase security role stress.

When information security policies do not clearly define the role each person should play and the superior’s order conflicts with the information security policies, employees experience a high level of security role stress. The observed conflicts and stress make employees aware that the information security policies are not effective and find out the vulnerability of the companies’ information security is high. However, because employees do not have sufficient security knowledge to estimate the damage that information securities will produce, employees under security role stress often underestimate the perceived severity of information security threats. Consequently we argue that

Hypothesis 3a. Security role stress will positively affect employees’ perceived vulnerability to information security threat.

Hypothesis 3b. Security role stress will negatively affect employees’ perceived severity to information security threat.

When employees’ security role stress is high, the company’s information security policies are perceived less effective. In such circumstances, employees may doubt the effectiveness of the response mechanisms and do not have confidence in responding to security threats. When employees experience security stress from the environment, they do not have much confidence in their own capability to implement the company’s information security policies. Therefore, we propose that
Hypothesis 4a. Security role stress will negatively affect employees’ perceived response efficacy to information security threat.

Hypothesis 4b. Security role stress will negatively affect employees’ perceived self-efficacy to information security threat.

With the continuous advancement of science and technology, the implementation of information security is getting more and more complex. In order to prevent potential loopholes and events of information security incidents, enterprises develop multiple security policies and regulations that require employees to comply (Higgins 1999). However, in the absence of education and training, security policies are complex and difficult to understand. Employees experience a high level of stress from the work environment. Such a high level of security task stress decreases employees’ task performance and negatively affects employees’ belief of their abilities to respond information security threats (AbuAlRub 2004; Yerkes and Dodson 1908). As a result, we argue that

Hypothesis 5a. Security task stress will negatively affect employees’ perceived response efficacy to information security threat.

Hypothesis 5b. Security task stress will negatively affect employees’ perceived self-efficacy to information security threat.

According to the protection motivation theory (Rogers, 1983), the result of coping appraisal is positively related to protection motivation. When employees are aware that the possibility of causing damage to information security and the extent of damage are high, employees tend to reinforce and improve information security to reduce damage. Therefore, we propose that.

Hypothesis 6a. Employees’ perceived vulnerability to information security threat will positively increase security compliance.

Hypothesis 6b. Employees’ perceived severity to information security threat will positively affect security compliance.

Under normal circumstances, when the implementation of security policies are perceived effective, employees are motivated to comply the security policies. In addition, appropriate education and training can enhance employees’ self-confidence in performing security-related tasks. Therefore, we assume that when the result of the process of coping appraisal is high, the level of compliance with the security policy will increase.

Hypothesis 7a. Employees’ perceived response efficacy to information security threat will positively affect security compliance.

Hypothesis 7b. Employees’ perceived self-efficacy to information security threat will positively affect security compliance.

Research Methodology

Research method and data collection

A survey is used to test the proposed model in this study. The survey items are referred from previous research, and a five-point Likert scale is used. The questionnaire were validated by MIS professor and industry professionals to reduce semantic ambiguity. The targeted participants are the employees who use computers at work. A snowball sampling strategy was used to collect the data. The participants were asked to invite their friends who are qualified to be our research subjects to join this study. The questionnaires were distributed through both online and offline channels.

Analysis and Results

Descriptive Statistics

In total, 379 responses were returned. After removing the invalid 55 responses, 324 data points were left. Among the 324 surveys, 269 responses were completed online and 55 came back on hard copies.
A T-test was done to check whether the two groups of questionnaires are significantly different. Since no significant difference was found, we combined these two groups of samples for the following statistical analysis. The demographics of the samples are summarized in Table 1.

<table>
<thead>
<tr>
<th>Measure</th>
<th>Category</th>
<th>Frequency</th>
<th>%</th>
<th>Category</th>
<th>Frequency</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Male</td>
<td>193</td>
<td>59.6</td>
<td>Female</td>
<td>131</td>
<td>40.4</td>
</tr>
<tr>
<td>Age</td>
<td>Less than 25</td>
<td>16</td>
<td>4.9</td>
<td>26-30</td>
<td>69</td>
<td>21.3</td>
</tr>
<tr>
<td></td>
<td>31-35</td>
<td>122</td>
<td>37.7</td>
<td>36-40</td>
<td>81</td>
<td>25.0</td>
</tr>
<tr>
<td></td>
<td>41-45</td>
<td>26</td>
<td>8.0</td>
<td>46-50</td>
<td>6</td>
<td>1.9</td>
</tr>
<tr>
<td></td>
<td>More than 51</td>
<td>4</td>
<td>1.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td>Ph. D.</td>
<td>13</td>
<td>4.0</td>
<td>Master’s Degree</td>
<td>128</td>
<td>39.5</td>
</tr>
<tr>
<td></td>
<td>College</td>
<td>168</td>
<td>51.9</td>
<td>Junior College</td>
<td>10</td>
<td>3.1</td>
</tr>
<tr>
<td></td>
<td>High school and blow</td>
<td>5</td>
<td>1.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occupation</td>
<td>Government Institutions</td>
<td>9</td>
<td>2.8</td>
<td>Information Technology</td>
<td>130</td>
<td>40.1</td>
</tr>
<tr>
<td></td>
<td>Finance</td>
<td>22</td>
<td>6.8</td>
<td>Service &amp; Retail</td>
<td>34</td>
<td>10.5</td>
</tr>
<tr>
<td></td>
<td>Education Service</td>
<td>10</td>
<td>3.1</td>
<td>Military Service</td>
<td>23</td>
<td>7.1</td>
</tr>
<tr>
<td></td>
<td>Transportation</td>
<td>7</td>
<td>2.2</td>
<td>Manufacturing</td>
<td>68</td>
<td>21.0</td>
</tr>
<tr>
<td></td>
<td>Construction</td>
<td>4</td>
<td>1.2</td>
<td>Medical</td>
<td>7</td>
<td>2.2</td>
</tr>
<tr>
<td></td>
<td>Others</td>
<td>10</td>
<td>3.1</td>
<td>Professions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Department</td>
<td>Human Resource</td>
<td>5</td>
<td>1.5</td>
<td>Engineering</td>
<td>4</td>
<td>1.2</td>
</tr>
<tr>
<td></td>
<td>Planning</td>
<td>16</td>
<td>4.9</td>
<td>Administration</td>
<td>27</td>
<td>8.3</td>
</tr>
<tr>
<td></td>
<td>Operation</td>
<td>1</td>
<td>0.3</td>
<td>Legal</td>
<td>2</td>
<td>0.6</td>
</tr>
<tr>
<td></td>
<td>Customer Service</td>
<td>3</td>
<td>0.9</td>
<td>R&amp;D</td>
<td>62</td>
<td>19.1</td>
</tr>
<tr>
<td></td>
<td>Accounting</td>
<td>14</td>
<td>4.3</td>
<td>Teaching</td>
<td>3</td>
<td>0.9</td>
</tr>
<tr>
<td></td>
<td>Design</td>
<td>2</td>
<td>0.6</td>
<td>Business</td>
<td>44</td>
<td>13.6</td>
</tr>
<tr>
<td></td>
<td>Information Tech.</td>
<td>118</td>
<td>36.4</td>
<td>Manufacturing</td>
<td>9</td>
<td>2.8</td>
</tr>
<tr>
<td></td>
<td>General Affairs</td>
<td>4</td>
<td>1.2</td>
<td>Others</td>
<td>10</td>
<td>3.1</td>
</tr>
<tr>
<td>Job Hierarchy</td>
<td>General Staff</td>
<td>235</td>
<td>72.5</td>
<td>First-line Supervisor</td>
<td>39</td>
<td>12.0</td>
</tr>
<tr>
<td></td>
<td>Department Manager</td>
<td>13</td>
<td>4</td>
<td>Middle Manager</td>
<td>27</td>
<td>8.3</td>
</tr>
<tr>
<td></td>
<td>Top Manager</td>
<td>10</td>
<td>3.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tenure</td>
<td>1-3 year(s)</td>
<td>141</td>
<td>43.5</td>
<td>4-6 years</td>
<td>70</td>
<td>21.6</td>
</tr>
<tr>
<td></td>
<td>7-9 years</td>
<td>55</td>
<td>17</td>
<td>10-12 years</td>
<td>29</td>
<td>9.0</td>
</tr>
<tr>
<td></td>
<td>More than 13 years</td>
<td>29</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of employees in the department</td>
<td>1-5</td>
<td>58</td>
<td>17.9</td>
<td>6-10</td>
<td>72</td>
<td>22.2</td>
</tr>
<tr>
<td></td>
<td>11-15</td>
<td>61</td>
<td>18.8</td>
<td>16-20</td>
<td>30</td>
<td>9.3</td>
</tr>
<tr>
<td></td>
<td>More than 20</td>
<td>103</td>
<td>31.8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of employees in the company</td>
<td>Less than 51</td>
<td>35</td>
<td>10.8</td>
<td>51-100</td>
<td>30</td>
<td>9.3</td>
</tr>
<tr>
<td></td>
<td>101-300</td>
<td>51</td>
<td>15.7</td>
<td>301-500</td>
<td>30</td>
<td>9.3</td>
</tr>
<tr>
<td></td>
<td>501-1000</td>
<td>27</td>
<td>8.3</td>
<td>More than 1000</td>
<td>151</td>
<td>46.6</td>
</tr>
</tbody>
</table>

Table 1. Demographic Information of the Participants (N=324)
The Measurement Model

Reliability and Validity

A bootstrap technique was adopted to process the analysis of measurement model. For internal consistency reliability, the values of Cronbach’s Alpha and composite reliability are suggested to be higher than 0.7; for convergent validity, the average variance extracted (AVE) for each construct is higher than 0.5 and the outer loading of each indicator is higher than 0.708 (Fornell and Larcker 1981). The results showed the AVE of complexity is only 0.272, thus it was abandoned. The AVE of “job insecurity” and “severity” are under 0.5, and the Cronbach’s Alpha or composite reliability value of “job insecurity”, “vulnerability”, and “severity” are under 0.7, therefore we examine the outer loading value of each indicator. The reliability and convergent validity are acceptable after two indicators in “job insecurity”, one indicator in “vulnerability”, and one indicator in “severity” were dropped. Table 2 reports the reliabilities and validity of the constructs.

Table 2. Reliabilities and Validity of the Constructs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Mean</th>
<th>Cronbach's Alpha</th>
<th>Composite Reliability</th>
<th>Average Variance Extracted (AVE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree of Freedom</td>
<td>2.71</td>
<td>0.795</td>
<td>0.878</td>
<td>0.707</td>
</tr>
<tr>
<td>Privacy Invasion</td>
<td>3.70</td>
<td>0.912</td>
<td>0.942</td>
<td>0.844</td>
</tr>
<tr>
<td>Job Insecurity</td>
<td>2.95</td>
<td>0.748</td>
<td>0.888</td>
<td>0.798</td>
</tr>
<tr>
<td>Role Conflict</td>
<td>2.67</td>
<td>0.827</td>
<td>0.862</td>
<td>0.613</td>
</tr>
<tr>
<td>Self-role distance</td>
<td>2.45</td>
<td>0.815</td>
<td>0.869</td>
<td>0.573</td>
</tr>
<tr>
<td>Role Ambiguity</td>
<td>2.53</td>
<td>0.907</td>
<td>0.928</td>
<td>0.684</td>
</tr>
<tr>
<td>Work Overload</td>
<td>2.77</td>
<td>0.894</td>
<td>0.914</td>
<td>0.730</td>
</tr>
<tr>
<td>Uncertainty</td>
<td>3.19</td>
<td>0.808</td>
<td>0.788</td>
<td>0.522</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>2.95</td>
<td>0.913</td>
<td>0.945</td>
<td>0.852</td>
</tr>
<tr>
<td>Severity</td>
<td>4.44</td>
<td>0.834</td>
<td>0.878</td>
<td>0.549</td>
</tr>
<tr>
<td>Response-efficacy</td>
<td>4.19</td>
<td>0.885</td>
<td>0.929</td>
<td>0.814</td>
</tr>
<tr>
<td>Self-efficacy</td>
<td>3.63</td>
<td>0.773</td>
<td>0.850</td>
<td>0.655</td>
</tr>
<tr>
<td>Security Compliance</td>
<td>4.27</td>
<td>0.900</td>
<td>0.937</td>
<td>0.833</td>
</tr>
</tbody>
</table>

In order to check whether the formation of second-order variable to achieve the validity of the satisfaction, we examined the loadings between first-order variable and second-order variable. It was found that the first-order variable for job insecurity was significantly lower for loading the second-order variable of security job stress. Therefore, we do not use job insecurity as one of the variables that form security job stress.

In addition, the discriminant validity was examined. The criteria is the square root of AVE for each potential variable must be greater than the correlation coefficient for the other different potential variables (Fornell and Larcker 1981). The results show that this study satisfies the condition of discriminant validity.

The Analysis of Structural Model

The software smartpls M3 was employed to test hypothesis and the structural model. The structural model is used to evaluating the path coefficients and R-square between the variables. Figure 2 illustrates the results of the structural model analysis of this study.
As indicated, security job stress significantly and positively affects security role stress (β = 0.455, p < 0.01, t = 7.95). This result confirms our expectations and provides support for hypothesis 1. Security task stress significantly and positively affects security role stress (β = 0.276, p < 0.01, t = 4.423), which confirms our expectations and provides support for hypothesis 2.

Security role stress affects vulnerability positively and significantly (β = 0.431, p < 0.01, t = 9.679). This result confirms our expectations and supports Hypothesis 3a. Besides, security role stress has a significant negative correlation with severity (β = -0.288, p < 0.01, t = 5.058). This result confirms what we expected, so hypothesis 3b is supported. Security role stress significantly and negatively affects response efficacy (β = -0.365, p < 0.01, t = 6.835), which confirms our expectations and provides support for hypothesis 4a. Meanwhile, security role stress significantly and negatively affects self-efficacy (β = -0.265, p < 0.01, t = 4.069), which confirms our expectations and provides support for hypothesis 4b.

Security task stress has a negative correlation with response efficacy (β = 0.214, p < 0.01, t = 2.664). This result is the opposite of what we expected, so hypothesis 5a is not supported. Security task stress has a positively weak correlation with self-efficacy (β = 0.102, p > 0.05, t = 1.289). The result does not meet our expectation and cannot provide support for hypothesis 5b.

Vulnerability affects security compliance negatively (β = -0.126, p < 0.01, t = 2.688). This result is the opposite of what we expected; thus, hypothesis 6a is not supported. Severity) has a significant correlation with security compliance positively (β = 0.269, p < 0.01, t = 5.132. This confirms our expectation and supports hypothesis 6b.

Response efficacy (β = 0.326, p < 0.01, t = 5.454) has a significant correlation with security compliance positively. This confirms our expectation and supports hypothesis 7a. Self-efficacy has a significant correlation with security compliance positively (β = 0.215, p < 0.01, t = 4.208). This confirms our expectation and supports hypothesis 7b.

**Discussion**

The purpose of this study is to extend PMT with stress perspective to find out how security-related stress impact information security compliance through protection motivation processes. The empirical results confirm all the hypotheses except H5a, H5b, and H6a. This study shows that security task stress not only has no negative correlation with response efficacy and self-efficacy, but also has a certain
degree of positive correlation. We observed that the level of security task stress of employees is relatively low compared with response efficacy and self-efficacy. The Inverted-U shaped effect of Yerkes & Dodson law (Yerkes and Dodson 1908) may be applied to explain the result. The negative correlation between vulnerability and security compliance also needs further interpretation. We argue that vulnerability may not be directly associated with the security compliance, and some mediating variables may exist.

This study explores the relationship between different types of stressors and protection motivation processes and shows important implications to academic researchers. The role of security role stress in the cognitive processes of threat appraisal and coping appraisal should be emphasized. Researchers may explore some intervention strategies to reduce the effect of security role stress in this process. Practitioners should define the roles and responsibilities clearly for employees enough of each member in information security policies to minimize role conflict or ambiguity. In addition, managers should work in line with the security policies to conflicting security requirements for employees.

References

Information Security Stress and Security Policy Compliance


