Received 20 October 2014
Revised 11 June 2015
24 August 2015
Accepted 24 August 2015



# Stress-based security compliance model – an exploratory study

Hiep-Cong Pham
*Department of Business Information Technology and Logistics, RMIT University Vietnam, Ho Chi Minh City, Vietnam*
Jamal El-Den
*School of Engineering and IT, Charles Darwin University, Darwin, Australia, and*
Joan Richardson
*Department of Business Information Technology and Logistics, RMIT University, Melbourne, Australia*

## Abstract

**Purpose** – This paper aims to extend current information security compliance research by adapting "work-stress model" of the extended Job Demands-Resources model to explore how security compliance demands, organization and personal resources influence end-user security compliance. The paper proposes that security compliance burnout and security engagement as the mediating factors between security compliance demands, organizational and personal resources and individual security compliance.

**Design/methodology/approach** – The authors used a multi-case in-depth interview method to explore the relevance and significance of security demands, organizational resources and personal resources on security compliance at work. Seventeen participants in three organizations including a bank, a university and an oil distribution company in Vietnam were interviewed during a four-month period.

**Findings** – The study identified three security demands, three security resources and two aspects of personal resources that influence security compliance. The study demonstrates that the security environment factors such as security demands and resources affected compliance burden and security engagement. Personal resources could play an integral role in moderating the impact of security environment on security compliance.

**Research limitations/implications** – The findings presented are not generalizable to the wider population of end-users in Vietnam due to the small sample size used in the interviews. Further quantitative studies need to measure the extent of each predictor on security compliance.

**Originality/value** – The originality of the research stems from proposing not only stress-based but also motivating factors from the security environment on security compliance. By using qualitative approach, the study provides more insight to understand the impact of the security environments on security compliance.

**Keywords** Compliance burnout, Job demands-resources, Security compliance, Security engagement, Security resources

**Paper type** Research paper

The authors would like to thank Editor-in-Chief Professor Steven Furnell and the two anonymous reviewers for their insightful comments and suggestions. The authors also would like to thank two PhD supervisors of the first author Professor Linda Brennan and Dr France Cheong at RMIT University for their valuable guidance in the early development stage of the paper idea and final refinement. Sincere thanks are due to all interviewees for their time and willingness to discuss their security experience so openly.

Information & Computer Security
Vol. 24 No. 4, 2016
pp. 326-347

2056-4961
DOI 10.1108/ICS-10-2014-0067

## Introduction

The risks to an organization's information resources are constantly growing due to rapid technological advances, such as Web 2.0. Loss of sensitive information continues to be a major concern for businesses' due to the ease of accessing information online. Organizations often implement a wide range of security measures to protect their digital resources and physical assets. As part of the overall security program, employees play key roles in reducing the risk to personal and enterprise-based information resources and assets. However, the majority of organizational security problems are indirectly caused by employees who violate or neglect to abide by information security measures in their organizations (Warkentin *et al.*, 2007). Employee attitudes, positive or negative, toward information security tasks either improve or detract from security compliance (Bulgurcu *et al.*, 2010; Colwill, 2009; Herath and Rao, 2009b).

Due to current volatility in the forms and patterns of information security risks, employees' awareness and security compliance procedures are integral to the development of effective business information security programs. The identification of personal and organizational factors that motivate individuals' security compliance is essential to the overall effectiveness of organizational security initiatives.

Research has shown that end-users are often the weakest link in an information security system (Crossler *et al.*, 2013). End-users may ignore organizational security policies and the associated business processes that ensure adherence to safe security practice. The results for businesses are incidents of unsafe security activities, such as downloading unverified software from the internet, using simple and obvious passwords and sharing computer accounts. Unsafe security acts have the potential to compromise the entire security system, despite the creation of sophisticated organizational security programs.

Prevention of end-users' security violations require more than the traditional technical security controls. To encourage security policy compliance (i.e. reducing internal security threats), organizations often introduce security trainings and communicate potential security risks to system users. Moreover, organizations can also enforce sanctions for security violations. Security trainings and security risk communications provide system users with necessary skills and knowledge to evaluate and respond to security threats (Cox, 2012; Furnell and Rajendran, 2012; Vance and Siponen, 2012; Vance *et al.*, 2012). The main premise is that people with better security skills and security risk awareness would be more likely to comply with security policies, and due to fear of strict sanctions, people would be less likely to violate security policies (Guo and Yuan, 2012; Vance and Siponen, 2012).

Security compliance cost has been recognized as a key factor that reduces security compliance (Padayachee, 2012; Ifinedo, 2011). Employees may find security compliance time-consuming and inconvenient, as it has the potential to obstruct their daily routine work. Difficulty in performing routine work tasks may negatively impact on employee compliance levels (Furnell and Rajendran, 2012; Vance and Siponen, 2012; Dhillon and Torkzadeh, 2006). D'Arcy *et al.* (2014) highlight the need to explore the negative impact of security requirements to compliance. Security tasks that cause stress and increase moral disengagement have been found to lead to security non-compliance (D'Arcy *et al.*, 2014).

This study aims to explore the impact of stress-based security requirements using the extended Job Demands-Resources (JD-R) model (Demerouti *et al.*, 2001) as the

theoretical basis. JD-R is a work-stress model that proposes job demands, and resources influence employees' organizational commitment and performance through job burnout and engagement, respectively (Crawford *et al.*, 2010; Demerouti *et al.*, 2001; Fernet *et al.*, 2013). Personal resources have been included in the extended JD-R model as a moderating factor in relation to the tension between demands, resources and burnout and engagement that influence the work environment, job performance, commitment and satisfaction (Bandura, 1997; Bakker *et al.*, 2010; Toner *et al.*, 2012). Based on the extended JD-R model, our study suggests that security compliance demands and organizational security resources affect system users' security compliance through compliance burnout and engagement. Personal security resources moderate the impact of the tension between security compliance demands and the provision of suitable resources on end-user's security compliance. JD-R model given its broad application provides no specific demands or resources that are relevant to a specific job context. Due to limited resources, organizations need to know specific security compliance demands and resources that are essential to increase security compliance activity. Equipped with that knowledge, organizations can focus their effort to develop security programs that encourage security compliance.

The study uses a qualitative approach to address the research problem. A lack of qualitative research investigating employee security compliance has been highlighted (Crossler *et al.*, 2013). Thus, this study explores insights into security compliance in actual work contexts to improve our understanding of security compliance.

First, the paper introduces a review of current approaches to enhance security compliance. Second, classification of security tasks is discussed. Third, we introduce a new security compliance model which incorporates security compliance demands, resources and end-users' personal security resources. Fourth, the findings of multi-case in-depth interviews are presented to further elaborate specific security demands and resources relevant to security compliance. Finally, future research directions are proposed.

## Review of security compliance behaviors

Traditionally, information security measures were designed to address four phases of organizational security risk (Warkentin and Willison, 2009):

(1) deterrence;
(2) prevention;
(3) detection; and
(4) recovery.

Information security compliance (from now on referred as security compliance) aims to improve the effectiveness of the "prevention" phase through improvements in end-user compliance. Security compliance research mostly addresses factors that affect employees' behavior when they do not follow their organizations' security policies or not demonstrate expected safe security behaviors.

General deterrence theory has been used mainly as a theoretical basis for understanding why employees follow (or do not follow) their organization's information security policies (Herath and Rao, 2009a; Hu *et al.*, 2011; Lee *et al.*, 2004). The use of punitive penalties and/or rewards is often used to achieve employees' desired behavior.

Fear of penalties and rewards for compliance or non-compliance have been found to have a significant impact on security behavior (Herath and Rao, 2009b; Kankanhalli *et al.*, 2003). As a result, communication of certainty and severity of penalties for rule-breaking behavior have been considered as effective strategies for the prevention of employee violations of security policies and required practices. However, the effectiveness of threats of punishment to force security compliance behaviors has been found to be debatable. Studies have reported inconsistencies in the impact of penalties and rewards as regulators of employees' security conduct (Cox, 2012; Dhillon and Mishra, 2007; Furnell and Rajendran, 2012; Hu *et al.*, 2011). The use of security compliance rewards and sanctions have been found to be ineffective because implementation of requisite security processes is practically difficult and often non-existent (Hu *et al.*, 2011; Guo and Yuan, 2012; Herath and Rao, 2009b).

Protection motivation theory (PMT) is a theory used to explain how security compliance is motivated by fear. PMT is a fear-based persuasive social communication tool which aims to influence cognition, attitudes, behavioral intentions and health behaviors (Maddux and Rogers, 1983; Rogers, 1975). Studies on the use of PMT in security compliance have shown that the level of evoked fear due to calculated evident security risk and the perceived effectiveness of the measures to prevent non-compliant security behavior have an influence on the adoption of requisite organizational security processes (Vance *et al.*, 2012; Ifinedo, 2011). There are some issues related to the effectiveness of using a fear-based approach. Poor security communications make it difficult for users to respond to possible but usually unlikely security threats. When the perceived direct costs to the users incurred from the security threat are lower than the indirect cost or effort required by the user to circumvent the threat, users can ignore security compliance requirements (Schneier, 2008). Often users can be motivated to respond to a security threat when the risk is evident. However, users do not feel personally at risk, and the risk can be difficult to be judged accurately due to inherent risk complexity, or heuristic factors such as optimism bias which make people consider risks are more likely to happen to others rather than themselves (Schneier, 2008; West, 2008). Moreover, Brennan and Binney (2010) stated that externally motivated fear and threat have a short-term motivating influence and are not self-sustaining.

Another approach to understand security compliance is drawn from the rational choice theory. Rational choice theory originally developed by Becker (1968) put forward two premises for the consideration of an offence:

(1) balancing of both costs and benefits of the offending; and

(2) the decision maker's perceived or subjective expectation of reward and cost.

Security tasks are regarded by employees as supportive tasks (secondary) to their main (primary) tasks. Employees' security compliance depends on the extent of the efforts or demands on work time he/she is required to exercise. Research has shown that the more employees are required to personally engage in fulfilling security tasks the less compliant they become (Adams and Sasse, 1999). For example, an end-user needs to copy a document to his/her portable USB. The company's information security policies require that the USB be scanned for infected viruses prior to performing the download. The end-user's primary task is to copy the document to the USB, and virus scanning on the USB is secondary. According to the rational choice theory (Becker, 1968), failure of the end-user to comply with the security policies on USB virus scanning is due to a

focus on the primary task at hand. The security policy represents an obstacle to the shortest path to the primary goal (Weirich and Sasse, 2001). Furthermore, the complexity, uncertainty and overload of security tasks were found to negatively affect security compliance (D'Arcy *et al.*, 2014). In other words, the nature of security tasks causes a certain level of stress and increases moral disengagement in the users which would then lead to non-compliance (D'Arcy *et al.*, 2014).

Consequently, when the security procedure interferes with the primary task, an end-user may ignore or even interfere with the security measures, as the end-user is more focused on the primary task and the associated rewards (Adams and Sasse, 1999). The burden of compliance with security tasks imposed on the end-users has been identified as one of the major factors leading to non-compliance (Vance and Siponen, 2012, Furnell and Rajendran, 2012).

## Stress-based security compliance

Employees are expected to comply with security policies and take good care of organizational information resources. Organizations are also expected to provide employees with clear security instructions, reasonable security responsibilities and resources to support security compliance. Security demands and resources impact on employees' security compliance. The following section provides an overview of the extended JD-R model to explain the mechanism of how security compliance demands, resources and personal security resources could impact on end-user security compliance.

The JD-R model classifies the work environment into two general categories, demands and resources specific to a work context (Demerouti *et al.*, 2001). The JD-R model explains that employee health and job performance can be affected by both positive (resources) and negative (demands) job characteristics via dual processes of burnout and engagement (Bakker and Demerouti, 2007). Job demands are associated with physical and/or psychological costs and are the main determinants of negative job strain (Demerouti *et al.*, 2009), depression and psychological distress (Bruck *et al.*, 2002). Job resources are those physical, social or organizational aspects of the job that help facilitate the fulfillment of goals, reduction of job demands' and associated physical and psychological costs and promotion of personal growth and development (Demerouti *et al.*, 2001). Job resources have been found to be positively associated with work motivation, organizational commitment and job engagement (Bakker *et al.*, 2003).

Burnout and engagement are the two key outcomes of the tension between job demands and resources. Burnout is a negative psychological state which is a direct outcome of job demands and can be mitigated by the provision of additional resources (Demerouti *et al.*, 2001). Burnout describes a state of mental weariness which includes two dimensions: exhaustion which is a measure of fatigue and cynicism which reflects a distant attitude toward work (Schaufeli and Bakker, 2004). Work engagement is a positive psychological component directly related to the provision of adequate job resources. Work engagement refers to a positive, fulfilling, work-related state of mind that comprises three psychological states (Schaufeli and Taris, 2014):

(1) vigor;
(2) dedication; and
(3) absorption.

Work engagement is considered as a motivational process created by job resources, and it mediates the impact of job demands and positively supports organizational outcomes (Schaufeli and Taris, 2014).

Personal strengths such as self-efficacy, esteem and optimism were incorporated in the JD-R model and found to mediate the impact of job resources and work engagement on employees' job performance (Xanthopoulou *et al.*, 2007). Research shows that personal strengths might have a moderating role in relation to the tension between demands, resources and perceived burnout (Bandura, 1997; Bakker *et al.*, 2010; Toner *et al.*, 2012).

Security tasks can be classified as routine or non-routine tasks that assure end-user adherence to organizational security policies and requisite practices. Routine security tasks are those undertaken by employees as part of their day-to-day activities. Routine security tasks can be simple or complex. Simple security compliance tasks can be completed by employees without much security knowledge. Such security tasks are simple and seamlessly embedded in work routines and processes, such as computer logoff or regular password. Complex security tasks require a certain level of end-user knowledge. Assessing security risks from email attachments or encrypting confidential information are examples of complex security processes that would require employee training. Security tasks become routine when employees find them essential, have the necessary skills to successfully complete the security process and have access to the resources required to fulfill the tasks.

Non-routine security tasks are those that the employees need to perform but may lack the requisite skills and view as inconvenient and an obstruction to their daily work. Keeping up with online security risks, or checking email authenticity are some examples of non-routine security tasks to some end-users. In other words, non-routine security tasks impose a burden on employees in terms of time and cognitive effort. It is important to the organization to identify the characteristics of security processes and employee attitudes that impact on the shift of a non-routine security task to the everyday embedded activity undertaken without effort by staff. The effectiveness of an organizational security program relies on whether the employees find the organization's expected security responsibilities seamless and meaningful (Dhillon and Torkzadeh, 2006).

Non-routine security tasks are considered to be a contributory cause of burnout to end-users, as fulfilling these tasks requires additional effort, and in most cases, the end-users need to have prior security knowledge and expertise. Organizational security programs need to distinguish between routine and non-routine security tasks so that suitable initiatives can be introduced to make non-routine become routine to the employee.

Organizational security resources provided to assist the end-users to comply with both routine and non-routine security tasks would reduce compliance burnout and increase security engagement. Security engagement refers the level of skill developments and moral commitment to the organization that end-users exercise in performing safe security practice.

In addition to supporting security resources, end-users need to use personal resources such as security self-efficacy to perform security tasks without experiencing compliance burnout. Security systems and business processes that are designed and

built with knowledge of security compliance burnout and security engagement are integral to the promotion of end-user security compliance.

## The research model

This research proposes that compliance with security tasks can cause compliance burnout to the end-users and can reduce their security compliance. On the other hand, organizational security resources provided to the end-users can reduce end-user compliance burnout and motivate users to engage in security activities. Security engagement is critical to sustained compliance, as the end-users need to be aware of the constant risks. Personal security resources can therefore act as a buffer to reduce the perceived compliance burnout and make security engagement more effective.

Figure 1 presents the conceptual research model that has been developed based on three predictor factors:

(1) security demands;

(2) organizational security resources; and

(3) personal security resources.

These factors are hypothesized to affect the employees' perceived security burnout and security engagement, which consequently affect security compliance. In particular, security demands are posited to increase the perception of security compliance burnout (*H1*). The provision of organizational resources helps to reduce the compliance burden and increase security engagement (*H2* and *H3*). Personal security strengths are posited to reduce security compliance burnout from complying with security demands (*H4*) and increase the effectiveness of security resources on security engagement (*H5*). Finally, the compliance burnout is expected to reduce security compliance (*H6*), whereas active security engagement is expected to increase security compliance (*H7*).

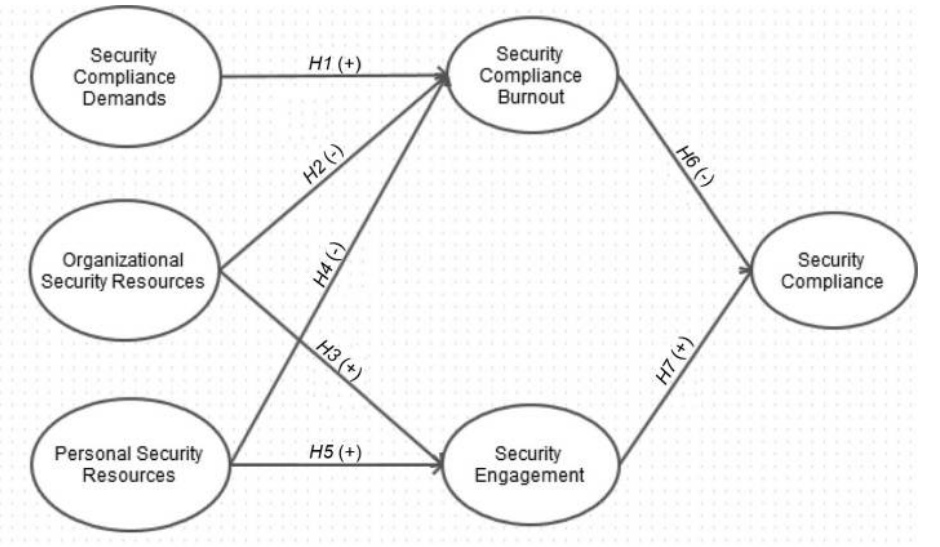


**Figure 1.**
Conceptual model of security compliance

## Research methodology

This study uses a multi-case study approach to explore what could make up the three factors in the conceptual model including security demands, organizational security resources and personal security resources. Case study approach is considered appropriate for studying a phenomenon in its natural settings where little or no previous research has been conducted (Pare, 2004). Little research has been conducted to explore characteristics of security compliance demands and resources that affect security compliance; the case study approach is therefore appropriate for this study. Case studies can be single or multi-case design where multi-case is mainly for replication purpose, not sampling logic (Yin, 2009). Multiple-case design increases the generalizability of research results by replicating the pattern matching in different cases. The IT security environment of organizations may vary in term of IT security demands and resources depending on their security risks, number of users, system complexity and many other characteristics. This explains why in this research, we adopted a multi-case design which included participants from different organizations in different industries to obtain diverse representation of the research findings. Further, the study focuses on exploring impacts of IT security environment on the system users; thus, only end-users from different departments were invited for interviews.

Given the typically small sample size of qualitative studies, informative cases are essential in answering research questions that meet the research objectives (Saunders *et al.*, 2012). In this study, it was important to choose organizations that used information technology intensively and expected the users to comply with security policies and/or practice. Diversity of the participants' job positions was also important to provide a range of employee views in relation to organizational security requirements. Organizations and participants for the interview were recruited through a network of alumni professionals who recommended suitable candidates for the study.

The candidate organizations were first screened to ensure they explicitly specified system users' security demands. Specification of security demands included formal policies such as written security policies, terms in labor contract or informal sources such as verbal instructions from IT department or supervisors. Examples of security specifications were conditions for accessing internet for work and non-work purposes, using portable devices at work or attending security training. As the main focus of the research questions was to explore the impact of security demands, organizational and personal resources on end-users' security compliance, participants were drawn from the end-user pool. No specific conditions were required for the participants, as long as they were willing to spend up to 60 min for the interviews at the organization's premise.

The interview questions were designed as open-ended and insight seeking to explore key security demands, organizational and personal resources which influenced participants' security compliance. The findings from one interview were used in the following interviews to enhance or explore further their meaning and implications to security compliance context. Also, through interviews new dimensions relating to security compliance emerged which could be significant in addressing the research questions and objectives.

Interviews were undertaken with 17 employees in three organizations during a four-month period. Initial data analysis after 17 interviews showed some level of theoretical saturation in which no major new security demands and resources were found. Ten bank clerks and a manager from a local bank branch, four lecturers and three

general staff from a local university and two marketing executives from an oil distribution organization in Hochiminh City, Vietnam, took part in 45-min long interviews. Table I describes the organizations and participants. The interviewed organizations were selected, as they had different security demands:

- the bank branch had clear security policies and enforced strict security compliance;
- the university had less restricted security policies and somewhat unclear security compliance demands; and
- the oil distribution company fell somehow in between.

These diverse security environments provided a range of security contexts for the study.

The interviews were conducted in both English and Vietnamese subject to the level of English competency of the participants and audio recorded for further analysis.

## Data analysis

Interview audio recordings were first transcribed by the researchers and stored in a file with an identifying label. Nvivo 10 was used to code participants' answers which were grouped by common key terms.

The interviews were conducted in both Vietnamese and English. The researcher then, translated the Vietnamese interviews into English. To ensure the accuracy of the translation, each transcript was verified by a qualified Vietnamese-English interpreter.

Interview data were categorized according to three sources (Strauss and Corbin, 1998):

(1) terms emerging from the data;

(2) the actual terms used by the participants, or

(3) terms used in existing theory and literature.

The main themes were pre-selected and included security demands, resources and compliance. These themes provided guidance for the data categorization process. To

| Organizations | System end-users | Participants | IT security systems |
|---|---|---|---|
| Local commercial bank branch (Organization A) | 30 | Six counter tellers<br>Two accountants<br>One branch manager | Firewalls, desktop security controls, limited internet access, proprietary banking system, IT helpdesk |
| Local university (Organization B) | 400 | Four academic staff, commerce and management department<br>Two professional staff from student service department | Proxy servers, desktop security controls, spam filtering, open internet access, IT helpdesk |
| International oil distribution (Organization C) | 80 | Two marketing executives from the marketing department | Desktop security controls, open internet access, IT helpdesk |

**Table I.**
Organizations and participant profiles

enhance reliability of the categorizing results, cross-verification of data coding was done with another IT expert.

The transcribed interview data were analyzed using a pattern matching and deductive analysis procedure proposed by Yin (2009). Before the interviews, research questions and broad themes had been developed from the literature. The interview data were then used to support and elaborate on the identified themes and to develop a more thorough explanation of the participants' experience of security compliance in organizations. The transcribed texts of all interviews were scanned to identify key words and important quotes that could support, explain or elaborate the identified themes. Categories that had not been identified in advance were still be recorded for further analysis and inclusion in the final theoretical model.

## Case analyses and findings

### *Security demands and compliance*

The participants were asked whether they experienced security compliance burnout at work and what security demands influenced their compliance burnout.

Participants at organizations B and C expressed a high level of mental fatigue while doing regular security tasks, such as changing passwords, periodical security auditing and requesting IT permission. Employees typically maintained multiple accounts (up to four accounts). The experience of security compliance burnout from bank participants was less obvious. Interviewed bank staff acknowledged the importance and necessity of maintaining security vigilance. For them, security requirements were clear and built in to work processes making compliance simple. Some bank staff emphasized that they did not have any problems following security measures, as they considered it an ethical responsibility toward the organization.

A bank staff member reflected on the compliance burnout issue:

> Personally, I don't think there is a burnout. The word that you used is quite strong, because this is also a job's responsibility. In certain job which requires information security, that is not considered burnout as it does not influence me that much. Security measures that I have to comply are quite simple and rarely happen so it doesn't matter much. (Organization A, counter teller 1).

A similar view was shared by the bank manager:

> For normal users, they are not active. They would just follow the regulation or instructions without any effort to achieve (Organization A, bank manager).

However, distant attitudes toward security compliance effort were evident among most participants. The majority of participants considered IT security the responsibility of the IT department. The participants were not concerned with common routine tasks, such as scanning viruses or contacting the IT department for help. However, when being asked to perform less common tasks, such as checking spoof emails or reading security warnings when opening an attachment, participants lacked sufficient knowledge to understand the risk associated with complex tasks.

Most participants emphasized that they needed to focus on their main job tasks rather than spending time or improving security knowledge and skills. Furthermore, technical restriction controls imposed on users' computers could further distance them from being more responsible for security compliance. Having less permission to do basic computer tasks made the participants less caring safe security practice.

In total, three main security demands emerged from the data that strongly affected the participants' compliance burnout:

(1) access to security policies;

(2) security compliance overload; and

(3) knowledge demand to comply with IT security requirements.

Each of the security demands is described in the following sections.

*Access to security policies.* In all three organizations, the main source of IT security requirements was the written IT policies which contained detailed instructions for proper security practice when dealing with confidential information, secure systems, company reputation and/or legal requirements. The length of IT policies in each organization varied from 5 to 15 pages.

Most participants were aware of the availability of the IT security policies but acknowledged that they just ignored or did not know where the policies were stored or that the policies were not disseminated by management. Employees admitted that written policies were of little use in the provision of the necessary knowledge to generate security compliance motivation. Almost all participants considered their organization's IT security policies as lengthy and difficult to read due to the use of unfamiliar terms. Documentation did not support compliance behavior. They associated their compliance knowledge to on-the-job knowledge, team sharing practice, instructions from direct supervisors and their general awareness of IT security purposes. As an academic staff commented:

> In the current organization I have not read much IT security policy because first it's too long, second it does not remind me of something. Currently I don't know whether we have a policy or it exists or not. I sometimes confused (Organization B, lecturer 2).

Another academic staff member highlighted the need to make IT policies more usable and accessible:

> We cannot remember all the policies and we just want to know those kinds of things that we deal every day or at least monthly. Those kinds of things should be easy to remember, in a friendly reminder mode, and for complicated policy, at least we know it exists and we can look for it. The frequencies that we work with those complicated policies may be not much, but at least we know they exist, and we can know who we can ask for them (Organization B, lecturer 5).

As the participants found existing IT security policies of little help in guiding security practice, other communications from the IT department were considered essential for maintaining security awareness. The participants emphasized that the IT department should communicate with staff regularly about the significance of IT security risks and the role of the end-users in the organizational picture. Without that information, the participants would at best passively comply or solely rely on the IT department to take care of organizational security.

*Security compliance overload.* One of the most common issues of security compliance demands was security compliance overload affecting the participants' main work and reducing productivity. It was common among the interviewed organizations to have multiple computer accounts for different systems with frequent password resets, regular system checkups and procedures to gain security access which added up to the frustration among the end-users.

Security compliance overload was expressed in term of time to comply and work obstructions affecting productivity. For example, an IT lecturer (Organization B, lecturer 5) explained that he had stopped changing one of the account passwords as required and resorted to downloading offline copies of documents rather than accessing them online. Another university lecturer (Organization B, lecturer 3) complained that frequent password changes (every three months) were unnecessary as there was no clear security risk. Remembering passwords became more difficult as there was a 15 iteration cycle for generating new passwords. The marketing executive (Organization C, staff 1) revealed she kept ignoring password change reminders until the last minute and was very concerned about the time-consuming work of security audit on her laptop.

Though most of the security tasks were completed by the IT department in each organization, the time it took employees to comply with these tasks affected their work productivity. Security demands such as scheduled IT equipment auditing and delay in processing software installation requests led to inconvenience and reduced productivity for the participants. Perceived IT security overload often became worse when the participants were not convinced of the positive impact of enforced procedures. A lecturer annoyed at the number of IT requests for minor software fixes commented that:

> I feel annoyed when I have to ask IT to come and authorise me to fix and install a common software. I think it needs to have room for the users to do it by themselves. There is certain software you can install by yourself (Organization B, lecturer 4).

Facing with increasing security demands, the participants seemed to develop workarounds. Skipping the tasks and/or failing to report IT security issues were options used to reduce the cost of compliance unless the tasks were made compulsory by the organization. A lecturer (Organization B, lecturer 4) raised the issue that due to strict IT security settings on staff computers, he was not able to use the software needed for his lecture. IT department assistance was not requested due to strict response time. A marketing officer (Organization C, staff 1) did not report initial problems on her laptop to IT department, as she was concerned at the amount of time it took to audit.

*Knowledge demand to comply with security requirements.* In terms of knowledge demand for IT security compliance tasks, most participants considered security compliance as relatively simple and straightforward. IT security compliance meant following routine technical control procedures for activities, such as changing passwords, locking up computers, virus protection or not sharing computer accounts. We noted that the increase in implementing technical controls in organizations made most of their IT security tasks easier and simpler for individual compliance. The marketing executive explained the difficulty of following IT security requirements as:

> The IT security measures are quite easy to follow, as long as I just follow instructions, not touching on the IT parts or as long as we don't make mistake on the IT things (Organization C, staff 2).

However, when being presented with three IT security scenarios, few participants expressed any interest to consult further IT security advice or had knowledge of inherent organizational risk in the depicted cases. Most participants did not know how to check a URL in an email for potential spoofing attacks by checking fake websites asking for personal information. IT security risk assessment for some staff was often too complex and/or time consuming. One staff member in the bank explained her view on security risk assessment:

> I can click on the warning message to cancel or run the application. But thinking about what IT security risks might happen if I run it would be too much to handle (Organization A, counter teller 3).

Similarly, the university student administrative staff member shared her view on skills required to evaluate security risks:

> It does not matter to me much as I don't have enough expertise and knowledge to assess the effectiveness of security tasks and the risks (Organization B, professional staff 1).

Most participants argued that the IT security knowledge required for security compliance by system users should be general and easy to comprehend and apply. Advanced knowledge required for security risk assessment, such as, reading complex instructions or regular skill updates should be for IT professionals and would not be in the interest of the participants.

*Organizational security resources and security compliance*

The participants were asked to explain which organizational resources helped reduce compliance burnout and increase security engagement. Overall, organizational resources were found essential to reduce individual compliance cost and encourage safe security practice. Security compliance engagement came in the form of willingness to learn security skills and to spend the time required to perform required security tasks. Security efforts including monitoring and reporting security incidents and taking personal responsibilities were integral to organizational security effectiveness.

Overall, most participants expressed little interest being involved with security activities at work. Participants did not want to put much effort into security except simple security routines.

One marketing executive explained her view on security engagement:

> I am not interested or find challenging for any of security tasks. I just find them obligations that I have to follow. It is just like a norm in the company. I just do it without any willingness or interest (Organization C, staff 1).

Interestingly, the same participant expressed interest in completing security training:

> I don't think we will be willing to spend time with security tasks. But we will be willing to spend time for some training or some visual learning from the security. It will be more interesting and we will be willing to (Organization C, staff 1).

The IT lecturer explained desirable security commitment:

> Security becomes something like when I want to do something, the first thing I think that I should check if we can do it or not. It will make like a culture that we ask the first question and we know where to check. And either my colleagues or I go to system to check and we know who should ask. and that
>
> They need to know what the environment they are working on, how much security to provide, what level of security they need to have and how they are going to protect themselves (Organization B, lecturer 5).

Three resources were found to strongly affect security compliance:

(1) organizational security response efficacies;

(2) individual compliance evaluation; and

(3) security compliance autonomy that provided opportunities to use and develop security skills.

Each of these resources is explained in the following sections.

*Organizational security response efficacy.* Most participants agreed that the IT department should be mainly responsible for managing IT security and should help end-users know what and how to comply with security requirements. Three IT response efficacies emerged from the data:

(1) timely and helpful IT support;

(2) IT staff competences; and

(3) evidence of IT value in the organization.

IT response efficacies were required to reduce the impact of IT security systems on employees' work by ensuring compliance time and effort were minimal. The participants expected minimum effort or involvement with security tasks. End-users expected timely and helpful responses from the IT department, simple explanations on complex security. With informative support the participants expressed willingness to engage in IT security practices. A lecturer explained how effective IT staff at work could encourage her compliance:

> Our IT staff's competencies are very important. They should be friendly, listening, and willing to help and giving advice beyond what people ask. Sometimes I have limited knowledge in IT or IT security, when I ask them I'm not sure it's right or not, so I think it's the way I need. But they should know more than me they can advise more than that (Organization B, lecturer 2).

Similarly, the marketing executive emphasized the importance of efficacy of the IT staff to her IT security compliance:

> I will take IT advice if the IT shows competency, capable of managing the IT security risks, and they give us some knowledge if we follow them. They have to demonstrate that they can do something with the risks for my computer first. From that I will take their advice into account. It should come from a qualified IT department, first of all (Organization C, staff 1).

Effective security support was clearly needed to reduce compliance cost, as one of the marketing executives emphasized the role of IT support and her security practice:

> The IT department is very helpful. I can seek for help from them any time I want. We hardly feel any compliance burnout except time. It's about attitude towards security tasks: security tasks are not my main tasks, it should take a small time of 8 hours in the office, or somehow we ignore it (Organization C, staff 1).

However, effective IT responses and minimal end-user security involvement can have a negative impact on compliance by developing over-reliance on IT staff for help with security issues. This may result in increased distance between end-users and security compliance. The most common IT security task that the participants reported completing was a simple report to the IT department for security help. Lack of self-efficacy and self-control in administering security settings for the employee's work were also quoted as reasons for underestimating the requirements of the personal compliance role and delegating tasks to the IT department. It was quite obvious that simply providing effective IT responses may not increase compliance, an additional set of resources may need to be deployed to increase end-users' compliance.

*Individual compliance evaluation.* Formal evaluation of individual IT security compliance was identified as an effective way to motivate on-going compliance though no interviewed organizations specified rewards or sanctions for individual compliance. Participants from the bank suggested a need for formal recognition, such as financial reward and/or performance bonus for individual IT security effort. In addition, compliance evaluation should also include penalties for non-compliance, such as losing a bonus, pay cut or even disciplinary actions. A bank staff member's suggestion for how to encourage IT security compliance effort in short term and long term was:

> But in short term, there should be a clear "award – punishment", gradually, it will become self-consciousness. In the long term, we will aim for the improvement in each individual's consciousness as if we require that from the beginning, that would be very difficult (Organization A, accountant 1).

Similarly, the marketing executive mentioned some forms of formal evaluation of IT security compliance effort:

> We need some award for staff to promote compliance. There is deviation report (something dangerous that may happen if we do something wrong), award (six month or a year) for a staff who follows or does well with the IT security compliance (Organization C, staff 1).

On the other hand, some participants did not recommend formal recognition for IT security compliance. These participants argued that IT security compliance was more as ethical duty and responsibility. According to these participants, IT security compliance was part of someone's job and should not be evaluated separately.

Financial reward was not the only form of recognition highlighted. Other forms of formal evaluation were also recommended. An academic staff suggested that IT security could be promoted as a mini competition among staff. Staff would document their own best IT security practice and compete against others for recognition of their effort. IT security competencies could be formally certified so that staff would know what level of awareness and skills were required for their job or indeed promotion.

The participants declared that formal evaluation of security compliance at work demonstrated the organizations took IT security seriously and that it was essential to the organization's wellbeing. The employees would only make IT security compliance a personal responsibility if the organization did so which required that IT security effort be recognized at different levels of achievements including non-achievement.

*Security compliance autonomy.* In total, 16 of 17 participants opted strongly for IT security programs that balanced between their work and their personal needs and provided some flexibility in IT settings. Six of nine participants from the bank, and all other participants were not satisfied with highly restricted IT security environments, removing most of their autonomy in deciding which software settings and applications to use for their work. IT security control inflexibility and strict control were perceived as hindrances for job performance and reduced productivity. A bank staff mentioned:

> I don't have much control over IT security as the company enforces strict IT security measures. I cannot access anything except work-related systems dictated by the IT department. Sometimes I feel frustrated as I can't access resources that are needed in my job (Organization A, counter teller 5).

A university lecturer desired customized security controls for different groups of users:

> I think it's good because the role of the users is different. People are teaching different courses and exposed to different kinds of teaching needs so I think we need to customise what the users need in term of security and protection (Organization B, lecturer 4).

The participants requested some sort of IT security-related decision autonomy which took into consideration their skills and expertise to improve IT security compliance. In the absence of compliance autonomy, the employees would comply passively and simply delegate security responsibility to the IT department, if possible. It is clear that the end-users would be more active and responsible for IT security if more self-control was provided by the organization. There was not much need for individual effort to improve knowledge and skills if they are not given opportunities to apply them. The marketing executive highlighted the need to use her computer skills in complying with security requirements:

> Matching computer skills will make me willing to comply. Security task could be personalized based on different requirements from different positions in the company (Organization C, staff 2).

Another member of bank staff highlighted lack of security compliance autonomy may even lead to intentional compromise of the IT security system:

> Regardless how restricted the IT security system is, someone still can get around it to access the resources they need. IT security measures should provide some flexibility to the staff in performing their job (Organization A, counter teller 5).

Interestingly, only a certain level of compliance autonomy was desired, as long as their job's needs were satisfactorily supported by the technology. Extra IT security compliance autonomy would just become a burnout especially when the participants were required to exercise extra effort and to make wise IT security decision in unclear situations. However, there was another view on the need to enable more IT security autonomy, if it did not necessitate extra responsibility but rather provided access to more resources to do one's job. As an end-user from the oil distribution organization highlighted, there was no need to have more responsibility for taking care of a computer or IT security. All that she needed was access to internet and run software that she needed.

*Personal security resources*

Interview data show that security self-efficacy and past security exposure are two main personal resources that affected security compliance. It was quite obvious that participants with more knowledge and IT general skills demonstrated a higher level of security awareness and confidence to deal with security risks. As one IT lecturer with good IT skills and knowledge clarified what one should do in regard to maintaining security compliance:

> They need to know what the environment they are working on, how much security to provide, what level of security they need to have and how they are going to protect themselves. And that […]

> Security becomes something like when I want to do something, the first thing I think that I should check if we can do it or not. It will make like a culture that we ask the first question and we know where to check. And either my colleagues or I go to system to check and we know who should ask (Organization B, lecturer 5).

Without appropriate security skills, it was difficult to make use of existing security resources. Some of the participants highlighted the need to have suitable security skills or expertise to make good use of the current security systems:

> It does not matter to me much as I do not have enough expertise and knowledge to assess the effectiveness of security tasks and the risks (Organization B, staff 2).

> Here we don't have IT background, most of us will just follow what the process or regulation request. For example we log in a program, we need an ID and password to do, most of us don't think about if we click the link, what may happen and what may influence the internet security. That is a little too much (Organization A, counter teller 4).

Experience of past security incidents strongly influenced participants' attitude toward security risks and security needs. These participants explained that past security exposure either through training or real incidents gave them the real experience of what a security risk could do to their digital assets and made them more personally cautious and willing to take extra effort and time to engage in security activities:

> If people can be educated to know what is virus, how it affects to your computer, something like that, and then next time, when people see about the virus, that word, then they will definitely be curious to know more about how it happens (Organization B, staff 2).

> I think that if we experience some problems before like losing the hard disk or losing the information, and corrupted […] I would be more cautious next time (Organization B, staff 2).

> We need mock up exercise through that we can find security compliance is very important and purposeful. Then we will follow actively and with supportive attitude (Organization C, staff 2).

## Discussion

The study identified three security demands, three organizational resources and two personal resources that affected security compliance burnout and engagement which eventually influenced security compliance.

This study also extends the current research on information security compliance by demonstrating that current implementations and operations of IT security systems have caused end-users' psychological burnout, thus making them less compliant or supportive to IT security measures. To increase employees' security compliance, organizations need to consider security initiatives that reduce burnout and enable security engagement through effective development of both security demands and provision of resources. Effective communication of security demands, minimizing time and effort of the end-users, identifying and providing necessary IT knowledge and establishing appropriate security compliance evaluation schemes are examples of such initiatives.

This study also raised several questions regarding alignment of organizational demands and resources to best achieve compliance and sustained commitment in information security contexts. Effective resources provided to end-users help reduce compliance burnout. However, heavily documented complex security policies can lead to over-reliance of the end-users on the IT department. End-users may find compliance less of a personal responsibility if the IT department acts as an effective safety net for information security assurance. Thus, to what extent compliance resources can be provided in conjunction with appropriate evaluation schemes requires further

exploration. Self-control or autonomy has been a key factor in behavioral theories that motivate people to adopt a behavior (Abrahama *et al.*, 1998; Vohs and Schmeichel, 2003). Similarly, in this study, compliance autonomy has been found to have strong influence on employee engagement with security activities. A balance between giving end-users sufficient security control to best fit their job requirements and minimizing human risks in security also needs to be better examined.

From a managerial perspective, this study provided a starting point for organizations to reconsider current information security programs. Understanding that compliance burnout from complying with security demands and active engagement with security activities are key to sustained compliance is the first step toward establishing an effective security program. Three security demand factors and three organizational resources identified in this study could serve as action plan for organizations. It is recommended based on our analysis that:

- Security practice should be effectively communicated in simple words together with graphical posters (e.g. using infographic), and reduce requests for end-users to refer to complex written security documents as their main source of instructions.
- IT security systems should be carefully reviewed to minimize the impact on employees' work productivity. Automation of routine security tasks should be conducted to reduce end-user involvement.
- Organizations should not rely on staff to expend extra effort in understanding and responding to standard security warnings. Risk information should be presented in simple, illustrative formats so that end-users can easily assess the severity of the risks through visual analysis.
- IT security measures should be effective, and technical supports are responsive and helpful to the users. Organizations should conduct end-user surveys to identify areas that need improvements and improve users' perception of organization's IT efficacies. Organizations should also consider customizing security controls for different groups of end-users to satisfy work needs and facilitate their ability to use and develop skills.
- Security compliance evaluation schemes should be established to reward and penalize individual security practice. Tangible or intangible rewards can be applied to recognize individual security effort or sanctions to deter serious non-compliance.

Though it is recommended that security compliance should not simply be promoted on an individual basis but to foster an organization-wide culture which could have significant impact to individuals' compliance (Lacey, 2010; Parsons *et al.*, 2010).

## Conclusion and future work

Effective security protection against security risks relies greatly on whether the end-users exercise safe security practice and obtain sufficient security knowledge. The end-users should be regarded as important assets and not just internal threats to the protection of organizational information assets. Our proposed security model moves away from traditional approaches which are mostly based on the use of formal sanctions and security fear-based communication, by considering employees' personal resources and the appropriate combination of security demands and organizational resources. We posit that organizations would increase security compliance by developing security policies and programs which could reduce compliance burnout and increase engagement by reducing

complex, overloading security demands and providing sufficient resources. We also argue that personal resources moderate the impact of the security demands and resources on perceived compliance burnout and security engagement.

Our study has qualitatively evaluated the proposed security compliance model with seventeen users in three organizations in Hochiminh City, Vietnam. Difficult access to security policies, security overload and high security knowledge demands could result in end-users' security burnout. Security resources, such as adequacy of organizational security resources, customized security self-control and individual security evaluation motivated the participants to get more involved with and take personal responsibility for security tasks. Lack of security engagement means the end-users simply delegated security responsibilities to the organization. Finally, personal resources including security self-efficacy and genuine experience could enhance security engagement through exploring new security techniques and giving moral support for organizational security effort.

The research has some limitations. In-depth interview method does not allow the model to be tested quantitatively to assess the extent of impact from the predictor variables such as security demands, security resources and personal resources to security compliance. More organizations in each industry should be interviewed to establish clearer picture of the security compliance in different environments. The next stage of the research would be to conduct a quantitative assessment of the model and enhance the explanatory power of the security compliance model in wider organizational contexts.

## References

Abrahama, C., Sheeranb, P. and Johnston, M. (1998), "From health beliefs to self-regulation: theoretical advances in the psychology of action control", *Psychology & Health*, Vol. 13 No. 4, pp. 569-591.

Adams, A. and Sasse, M.A. (1999), "Users are not the enemy", *Communications of the ACM*, Vol. 42 No. 12, pp. 40-46.

Bakker, A.B., Boyd, C.M., Dollard, M., Gillespie, N., Winefield, A.H. and Stough, C. (2010), "The role of personality in the job demands-resources model: a study of Australian academic staff", *Career Development International*, Vol. 15 No. 7.

Bakker, A.B. and Demerouti, E. (2007), "The job demands-resources model: state of the art", *Journal of Managerial Psychology*, Vol. 22 No. 3, pp. 309-328.

Bakker, A.B., Demerouti, E. and Schaufeli, W.B. (2003), "Dual processes at work in a call centre: an application of the Job Demands-Resources Model", *European Journal of Work and Organizational Psychology*, Vol. 12 No. 4, pp. 393-417.

Bandura, A. (1997), *Self-Efficacy: The Exercise of Control*, Freeman, New York, NY.

Becker, G.S. (1968), "Crime and punishment: an economic approach", *Journal of Political Economy*, Vol. 76 No. 2.

Brennan, L. and Binney, W. (2010), "Fear, guilt and shame appeals in social marketing", *Journal of Business Research*, Vol. 63 No. 2, pp. 140-146.

Bruck, C.S., Allen, T.D. and Spector, P.E. (2002), "The relation between work-family conflict and job satisfaction: a finer-grained analysis", *Journal of Vocational Behavior*, Vol. 60, pp. 336-353.

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*, Vol. 34 No. 3, pp. 523-548.

Colwill, C. (2009), "Human factors in information security: the insider threat - who can you trust these days?", *Information Security Technical Report*, Vol. 14 No. 4, pp. 186-196.

Cox, J. (2012), "Information systems user security: a structured model of the knowing – doing gap", *Computers in Human Behavior*, Vol. 28 No. 5, pp. 1849-1858.

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*, Vol. 95 No. 5, pp. 834-848.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hud, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computer & Security*, Vol. 32 No. 1, pp. 90-101.

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*, Vol. 31 No. 2, pp. 285-318.

Demerouti, E., Bakker, A.B., Nachreiner, F. and Schaufeli, W.B. (2001), "The job demands-resources model of burnout", *Journal of Applied Psychology*, Vol. 86 No. 3, pp. 499-512.

Demerouti, E., Le Blanc, P.M., Bakker, A.B., Schaufeli, W.B. and Hox, J.(2009), "Present but sick: a three-wave study on job demands, presenteeism and burnout", *Career Development International*, Vol. 14, pp. 50-68.

Dhillon, G. and Mishra, S. (2007), "Information systems security governance research: a behavioral perspective", 2nd Annual Symposium on Information Assurance, New York, NY.

Dhillon, G. and Torkzadeh, G. (2006), "Value-focused assessment of information system security in organizations", *Information Systems*, Vol. 16 No. 3, pp. 293-314.

Weirich, D. and Sasse, M.A. (2001), "Pretty good persuasion: a first step towards effective password security for the real world", *The New Security Paradigms Workshop*, Cloudcroft, NM, pp. 137-143.

Fernet, C., Austin, S.P., Tre′panier, S.-G.V. and Dussault, M. (2013), "How do job characteristics contribute to burnout? Exploring the distinct mediating roles of perceived autonomy, competence, and relatedness", *European Journal of Work and Organizational Psychology*, Vol. 22 No. 2, pp. 123-137.

Furnell, S. and Rajendran, A. (2012a), "Understanding the influences on information security behavior", *Computer Fraud & Security*, Vol. 2012 No. 3, pp. 12-15.

Guo, K.H. and Yuan, Y. (2012), "The effects of multilevel sanctions on information security violations: a mediating model", *Information & Management*, Vol. 49 No. 6, pp. 320-326.

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

Herath, T. and Rao, H.R. (2009b), "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165.

Hu, Q., Xu, Z.C., Dinev, T. and Ling, H. (2011), "Does deterrence work in reducing information security policy abuse by employees?", *Communications of the ACM*, Vol. 54, pp. 54-60.

Ifinedo, P. (2011), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers & Security* Vol. 31 No. 1, pp. 83-95.

Kankanhalli, A., Teo, H.-H., Tan, B.C.Y. and Wei, K.-K. (2003), "An integrative study of information systems security effectiveness", *International Journal of Information Management*, Vol. 23 No. 2, pp. 139-154.

Lacey, D. (2010), "Understanding and transforming organizational security culture", *Information Management & Computer Security*, Vol. 18 No. 1, pp. 4-13.

Lee, S.M., Lee, S.-G. and Yoo, S. (2004), "An integrative model of computer abuse based on social control and general deterrence theories", *Information & Management*, Vol. 41 No. 6, pp. 707-718.

Maddux, J.E. and Rogers, R.W. (1983), "Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change", *Journal of Experimental Social Psychology*, Vol. 19 No. 5, pp. 469-479.

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

Pare, G. (2004), "Investigating information systems with positivist case study research", *Communications of the AIS*, Vol. 13, pp. 233-264.

Parsons, K., Mccormac, A., Butavicius, M. and Ferguson, L. (2010), "Human factors and information security: individual, culture and security environment", in Defence, A.D.O. (Ed.), *DSTO Defence Science and Technology Organisation*, Edinburgh.

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

Saunders, M., Lewis, P. and Thornhill, A. (2012), *Research Methods for Business Students*, Pearson Education, Upper Saddle River, NJ.

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 Orgnizational Behavior*, Vol. 25 No. 3, pp. 293-315.

Schaufeli, W.B. and Taris, T.W. (2014), "A critical review of job demands-resources model: Implications for improving work and health", in Bauer, G.F. and Hammig, O. (Eds), *Bridging Occupational, Organizational and Public Health: A Transdisciplinary Approach*, Springer Science+Business, Dordrecht.

Schneier, B. (2008), "The psychology of security", available at: www.schneier.com/essay-155.html, www.schneier.com/essay-155.html (accessed 20 July 2013).

Strauss, A. and Corbin, J. (1998), *Basics of Qualitative Research*, Sage, Thousand Oaks, CA.

Toner, E., Haslam, N., Robinson, J. and Williams, P. (2012), "Character strengths and wellbeing in adolescence: structure and correlates of the values in action inventory of strengths for children", *Personality and Individual Differences*, Vol. 52 No. 5, pp. 637-642.

Vance, A. and Siponen, M. (2012), "Is security policy violations: a rational choice perspective", *Journal of Organizational and End User Computing*, Vol. 24 No. 1, pp. 21-41.

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating is security compliance: insights from habit and protection motivation theory", *Information & Management*, Vol. 49 Nos 3/4, pp. 190-198.

Vohs, K.D. and Schmeichel, B.J. (2003), "Self-regulation and the extended now: controlling the self alters the subjective experience of time", *Journal of Personality and Social Psychology*, Vol. 85 No. 2, pp. 217-230.

Warkentin, M., Shropshire, J. and Johnson, A. (2007), "The IT security adoption conundrum: an initial step towards validation of applicable measures", *Proceedings of the 13th Americas Conference on Information Systems*, *Keystone, CO*.

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.

West, R. (2008), "The psychology of security: why do good users make bad decisions?", *Communications of the ACM*, Vol. 51 No. 4, pp. 34-40.

Xanthopoulou, D., Bakker, A.B., Demerouti, E. and Schaufeli, W.B. (2007), "The role of personal resources in the job demands-resources model", *International Journal of Stress Management*, Vol. 14 No. 2, pp. 121-141.

Yin, R.K. (2009), *Case study research: Design and Methods*, Sage, Thousand Oaks, CA.

## About the authors

Hiep Cong Pham is a Senior Lecturer in the Department of Business Information Technology and Logistics at RMIT University, Vietnam, where he has been a faculty member since 2008. Hiep has been working on his PhD in the area of information security compliance. Hiep Cong Pham is the corresponding author and can be contacted at: hiep.pham@rmit.edu.vn

Jamal El-Den is a Senior Research Fellow at Charles Darwin University, School of Engineering and IT. Dr El-Den received a PhD from the University of Technology, Sydney, Australia in IT/IS. He has been in academia for over 30 years at different institutions in Australia and overseas. Dr El-Den's main research interests are in knowledge management, knowledge sharing, organizational learning and positive psychology. He has more than 40 journals and conferences publications. He has established research groups in China and Vietnam. He is a supervisor of PhD and Masters students in the area of his research.

Joan Richardson is an Associate Professor in the Department of Business Information Technology and Logistics at RMIT University, Australia. She won an ALTC citation (2011) that recognized her particular contribution to improving student satisfaction and student engagement through the use of emerging technologies in Digital Literacy curriculum. In addition, she has worked extensively with Pearson Education Australia as the principal author for texts, e-texts and multi-media resource libraries since 2000. Innovations include the use of social networking features to enable peer engagement, SMS to disseminate assessment reminders and performance feedback, websites, multi-choice tests and communications sent from the learning management systems to personal mobile devices. Her substantial record of Information Systems (IS) research also includes six PhD completions and more than 75 peer reviewed book chapters, journals and conference publications. She presents her research publications and professional achievements, such as accreditation documentation addressing the Skills For the Information Age (SFIA) framework at national and international conferences. Her personal commitment to learning and teaching quality has been demonstrated by involvement in activities, such as externally funded projects, publication and Chairing the Victorian branch of HERDSA. She has been an Associate Editor of the *HERDSA* journal and participated in an ALTC project, entitled "Web 2.0 authoring tools in higher education learning and teaching: New directions for assessment and academic integrity".