# INFLUENCE OF SECURITY COMPLIANCE DEMANDS AND RESOURCES ON SECURITY COMPLIANCE-AN EXPLORATORY STUDY IN VIETNAM

Cong Hiep Pham, School of Business Information Technology and Logistics, RMIT University Vietnam, Vietnam, hiep.pham@rmit.edu.vn

Jamal El-den, Charles Darwin University, Darwin, Australia, jamal.ed-den@cdu.edu.au

Joan Richardson, School of Business Information Technology and Logistics, RMIT University, Melbourne, Australia, joan.richardson@rmit.edu.au

## Abstract

*This study extends current information security compliance research by adapting "work-stress model" of the Job Demands-Resources (JD-R) model to explore how security compliance demands and security resources influence the system users' information security compliance. The paper proposes that security compliance burnout and security engagement as the mediating factors between security compliance demands, security resources and individual security compliance. We employed a multi-case study method to explore the characteristics of security compliance demands and security resources that could influence security compliance. Interviews with system users in three organisations in Vietnam revealed three types of security compliance and four types of security resources that may influence security compliance burnout and engagement respectively. Practical implications of the initial findings are also presented.*

*Keywords: Security compliance, Compliance burnout, Security engagement, Security demands, Security resources.*

# 1 INTRODUCTION

The term "information security" refers to protecting data and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to ensure their confidentiality, integrity and availability (US Code Title 44, Chapter 35, Subchapter III, § 3542). Information security threats are major concerns for organisations that rely on networked information systems to store corporate information and to conduct essential business functions. Information security threats can be external or internal and threaten the confidentiality, integrity and availability of the organisational information and information systems. External security threats can be viruses; malwares, or professional hackers, whereas, internal security threats mostly come from employees. The employees may intentionally or unintentionally violate security procedures and may inflict severe damages to the organisations' information.

Organisations often implement technical security protection measures and use security policies as instructions and guidance for their employees to practice safe security practice to protect information security. Research has shown that system users are often the weakest link in IT security systems (Crossler et al. 2013). Organisations lose millions of dollars due to their employees' negligence and non-compliance in information security and that 60% of IT managers of global companies reported employees' misconduct as the real threats to information security (Herath and Rao 2009a) . For a number of reasons, system users may ignore adhering to safe security practices as specified in the security policies, for example installing free software from the Internet, using simple passwords, or sharing computer accounts. Unsafe security practice could compromise the whole security system regardless of how sophisticated and effective technical security protection measures are.

Prevention of system users' security violations requires more than the traditional technical security controls. To encourage security policy compliance (i.e. reducing internal security threats), organisations often introduce security trainings and communicate potential security risks to system users. Moreover, organisations 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 recognised as a key factor that reduces security compliance (Padayachee 2012, Ifinedo 2011). Employees may find security compliance time-consuming and inconvenient and obstructing their daily routine work and may not comply anymore (Furnell and Rajendran 2012, Vance and Siponen 2012, Dhillon and Torkzadeh 2006). Recent study showed that security tasks could cause stress, incease moral disengagement, and lead to security non-compliance (D'Arcy et al. 2014). D'Arcy et al. (2014) highlight the need to explore the negative impact of security requirements to security compliance.

This study examines stress-based factors to security compliance, however, from a different perspective. Job Demands-Resources (JD-R) model (Demerouti et al. 2001) is a work-stress model that proposes job demands and job resources influence employees' organisational commitment and performance through job burnout and job engagement respectively (Crawford et al. 2010, Demerouti et al. 2001, Dwyer and Ganster 1991, Fernet et al. 2013). Based on the JD-R model, our study suggests that security compliance demands and organisational security resources affect system users' security compliance through compliance burnout and engagement. Given their limited resources, organisations need to know specific security compliance demands and resources that are most essential to increase security compliance. Equipped with that knowledge, organisations can focus their effort to develop security programs that can reduce compliance burnout and increase security compliance engagement.

This study aims to identify some of the security compliance demands and security resources which might affect security compliance. The study employs a qualitative approach to answer the research questions. Lack of qualitative research in security compliance has been highlighted and more insights of security compliance should be explored in actual work contexts (Crossler et al. 2013). Thus this study contributes to explore insights into security compliance behaviour and improve understanding of security compliance.

The remainder of the paper is structured as follows. Firstly, literature review of current IT security compliance approaches is presented. Secondly, the JD-R model is explained as a theoretical basis to understand two motivational outcomes of security compliance under security compliance demands and organisational resources. Next, justification of the study's research methodology followed by the initial research findings, practical implications of the study model are presented.

# 2 CURRENT APPROACHES TO MOTIVATE SECURITY COMPLIANCE

Security non-compliance can be classified as intentional or unintentional computer violations (Padayachee 2012). Intentional computer violations can be further divided into malicious or non-malicious violations. Malicious intentional violations involve a premeditated intention to harm the company's information and computer resources for revenge or commercial gains (Lee et al. 2004, Hu et al. 2011, Hovav and D'Arcy 2012). Non-malicious intentional violations may involve unsafe IT security practice to save time for personal convenience (Vance and Siponen 2012). Unintentional violations occur could be due to lack of security awareness or knowledge of security policies implemented in the company. For example, an employee may install a freeware on an office computer without realising that the freeware could spread malware or viruses to the organisational network and its computers.

Behavioural theories have been employed to understand why employees comply and/or do not comply with IT security requirements. Treating non-compliance as intentional violations, preventive theories such as General Deterrence theory introduces sanctions and rewards to deter and reduce security violations (Herath and Rao 2009a, Hovav and D'Arcy 2012, Hu et al. 2011). Fear of sanctions for non-compliance and rewards for compliance have been found to have a significant impact on IT security behaviour (Herath and Rao 2009b, Kankanhalli et al. 2003). Thus communication of certainty and severity of sanctions for non-compliance could be effective in preventing employees from violating IT security policies.

Motivation to comply with IT security policies can be affected by perceived fear of the security threats' consequences. Fear-based theories such as Protection Motivation Theory (PMT) have been widely used to explain the impact of perceived fear of security threats on compliance. PMT explains that people are motivated to take protective actions to reduce fear as a result of conducting security threat appraisal and response appraisal (Maddux and Rogers 1983, Rogers 1975). Perceived fear of security risk consequences would motivate system users to take counter-measures to reduce such fear if only effective response measures are available and people are capable of taking them (Vance et al. 2012, Ifinedo 2011).

Security compliance can also be examined from a rational cost-benefit analysis. Rational choice theory (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 expectation of reward and cost of not committing an offence. For example, a user may avoid scanning a USB to save time but need to balance with the cost of losing stored data on the device. Immediate and direct cost of security compliance has been recognised as a key factor that reduces security compliance (Padayachee 2012, Ifinedo 2011). Employees may find security compliance time-consuming and inconvenient and obstructing their daily routine work. Research has shown that when security measures hinder the employees from doing their job, they start to get around it or stop complying with security measures (Furnell and Rajendran 2012, Vance and Siponen 2012, Dhillon and Torkzadeh 2006). Furthermore, the complexity, uncertainty, and overload of security tasks were found negatively affecting security compliance (D'Arcy et al. 2014). Such nature of security tasks causes certain level

of stress and increase moral disengagement in the users which would then lead to non-compliance (D'Arcy et al. 2014).

The current study follows the research direction of exploring security compliance cost and how it affects security compliance. The next section provides the theoretical basis of the study model.

# 3 SECURITY COMPLIANCE DEMANDS, RESOURCES AND SECURITY COMPLIANCE

Job Demands-Resources (JD-R) model is a work stress model which explains employees' job commitment and job performance can be affected by both positive (resources) and negative (demands) job characteristics via dual processes of job burnout and engagement (Bakker and Demerouti 2007). Job demands associated with both physical and psychological cost of the job have been identified as the main determinants of negative job strain (Demerouti et al. 2009), depression and psychological distress (Bruck et al. 2002). Job resources, on the other hand, are those physical, social, or organisational aspects of the job that help facilitate the fulfilment of goals, reduction of job demands' associated physical and psychological costs, and promotion of personal growth and development (Demerouti et al, 2001).

Job burnout is a state of mental fatigue including exhaustion and cynicism (Schaufeli and Bakker 2004) which is a direct outcome of certain job demands and can be mitigated by job resources (Demerouti et al, 2001). Whereas job engagement is a positive, fulfilling, work-related state of mind as a result of receiving adequate job resources that support the achievement of work goals or satisfaction of basic needs (Schaufeli and Taris, 2014). Job engagement can also be characterised as level of energy, involvement and efficacy one has in performing a job (Schaufeli et al. 1996). Job engagement has been found increasing job commitment, job satisfaction and individual performance.

Organisations require employees to comply with IT security policies and to take cautious IT security care when dealing with organisational information resources. Security measures often add extra overhead such as compliance time and knowledge demand on the system users to comply. Security tasks and the impact of fulfilling security tasks on system users' work can be considered as security compliance demands. Security compliance demands can lead to compliance burnout and reduce security compliance. In the meantime, organisational security resources such as clear security policies, security awareness trainings and regular technical support can help system users to fulfil security demands by reducing compliance burnout and increase engagement.

This study proposes that system users who have to adhere to stressful security demands experience compliance burnout (H1) which then reduces their security compliance (H4). Receiving relevant organisational supporting resources to promote security compliance would reduce the compliance burnout (H2) and increase compliance engagement (H3), which then increase security compliance (H5) (see Figure 1 for the conceptual security compliance model).

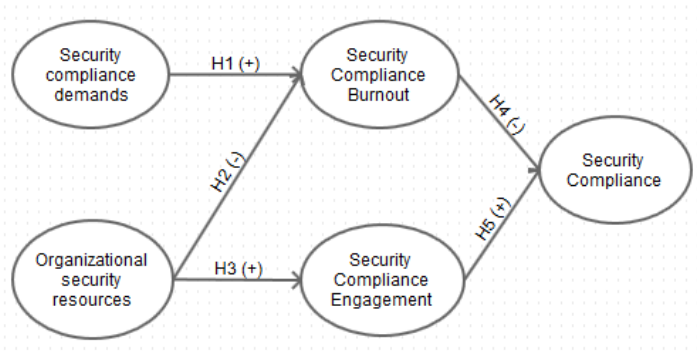


*Figure 1: Conceptual security compliance model*

JD-R model is an open and descriptive model which does not specify well-defined sets of job demands, resources, and organisational outcomes (Schaufeli and Taris, 2014). In particular, JD-R model does not specify what demands or resources would be the source(s) of employees' stress and/or effectively reducing job demands' stress as well as enhancing job engagement in a specific work environment. Though a comprehensive list of job demands and resources have been developed in Schaufeli and Taris (2014), it has little value to organisations to focus on all demands and resources to improve security compliance. Thus, the study is designed to to explore security compliance demands and resources that might influence security compliance through security compliance burnout and security engagement.

# 4 RESEARCH DESIGN AND METHODOLOGY

This study employs a multi-case study approach to address the research problem. Case study approach is considered appropriate for studying a phenomenon in its natural settings where little or no previous research has been done (Pare 2004). Little research has been conducted to explore characteristics of security compliance demands and resources that affect security compliance; case study method is suitable 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 generalisability of research results by replicating the pattern matching in different cases. IT security environment of an organisation 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 includes participants from different organisations in different industries in order 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 system 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 and to meet research objectives (Saunders et al. 2012). In this study, it was important to choose organisations that used information technology intensively and expected the users to comply with security policies. Diversity of the participants' job positions was also important to provide diverse views of their security experience. Organisations and participants for the interview were recruited through a network of friends and colleagues who recommended suitable candidates for the study.

The candidate organisations were first screened to ensure they explicitly specified system users' security responsibilities. Specification of security responsibilities could be formal such as written security policies, terms in labour contract or informal such as verbal instructions from IT department or supervisors. Examples of security specifications could be conditions of accessing Internet for work and non-work purposes, using portable devices at work, or attending security trainings. Security specifications were collected during the interview to rate the level of security demands in each interviewed organisation. As the main focus of the research questions are to explore the impacts of security environment on system users' security compliance, only system users were invited for interviews. No specific conditions were required for the participants so as long as they were willing to spend up to 60 minutes for the interviews at the organisational premise.

Interviews were undertaken with seventeen people in three organisations during a four-month period. The interviewed organisations including a local bank branch, a university, and an oil distribution firm were selected as they had different security demands and security resources which provided diverse security contexts for the study.

# 5 INITIAL FINDINGS

Due to page numbers limit of the paper, only a summary of the results is presenten in the paper. In total, three security demands and four security resources were identified from the interview data that affected the participants' security compliance. The three security demands are the need to learn security policies, security skill demand to comply with security requirements, and security compliance overload. The four organisational security resources are organisational security response efficacies,

level of security compliance autonomy, opportunities to develop security skills, and individual compliance evaluation.

Based on the initial findings, an updated security compliance model is proposed (Figure 2).

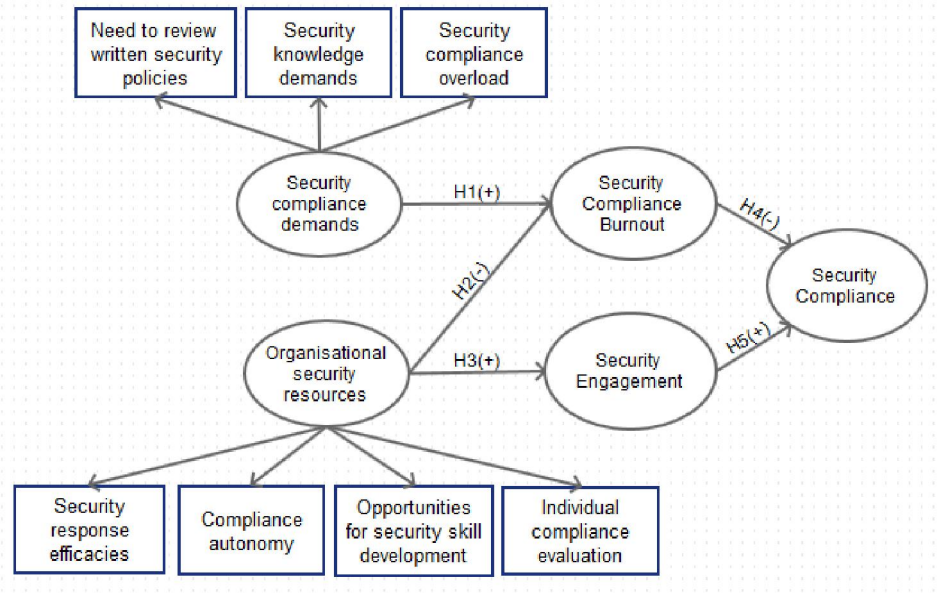


*Figure 2: Updated security compliance model*

The following section briefly discusses the initial findings of the study.

Question 1: What security demands affect security compliance?

The interview data revealed that not all participants experienced security compliance burnout from routine security demands at work. Especially participants from the bank branch even though they had to comply with much stricter security demands. Most participants considered security tasks demands as simple and easy to comply with. However, compliance burnout would increase sharply when the participants had to comply with more complex security tasks such as reading security policies for instructions, acquiring specific knowledge of emergent security risks (e.g. spoofing websites) or to assess unfamiliar security risks, or complying with security tasks which interfere with their main jobs.

Most participants emphasised that the organisation should communicate security policies in a fun, simple, and easy to comprehend. The current written format of the security policies really discouraged them from being more active compliance. On the exception of the IT lecturer, all other participants reported little or no IT knowledge which might help them to understand the contents of the security policies and stated that it was too much additional work to adhere to all security requirements in their work. Compliance burnout would also increase when the participants are not well informed and clear about the purpose of the security measures implemented. Interview data shows that if system users experience overloading or counterproductive security measures and become cynical toward overall organisational security effort they would avoid or delay complying with security tasks.

It is interesting to notice that having experienced less compliance burnout does not always lead to higher compliance. People may not experience burnout simply because they do not have to be involved with security tasks or delegate security tasks to the organisation. Active involvement of the users is required and the security risk levels need to be communicated regularly to remind of the need to be aware of the risks and that the users can play an important role to protect organisational security.

Question 2: What organisational resources affect security compliance?

Based on the interview findings, organisational security resources including organisational security response efficacies, opportunities to develop skills, compliance autonomy, and personal compliance evaluation (i.e. rewards and sanctions) are found to affect security compliance. Firstly, the participants expected that the organisation must demonstrate competences of providing security tools and support system users in their daily work. It is then the participants would take part in the security program. Secondly, good security compliance means security competency and that security skills should be treated as a necessary work attribute. This would result in compliance diligence without experiencing compliance burnout. Thirdly, due to the nature of security controls, users often have little control in what to do with security and increase their frustration, especially when adherence of security controls affects work productivity. If security policies that are not built to accommodate for system users' prior security expertise could frustrate them as they cannot use their skills that could further discourage system users from active compliance. Organisation should allow appropriate security compliance autonomy that can encourage system users to be more responsible as they can use their skills. Lastly, most participants treated security compliance tasks as additional and unnecessary and should be minimised. However, some participants expressed that they would be more willing to enhance their security skills and pay attention to security if personal compliance evaluation was implemented. For example, security skills and active compliance should be recognised, rewarded or poor compliance should be penalised.

Though little evidence of compliance engagement was found among the participants, the highly engaged participants often have prior security knowledge, have good knowledge of security requirements and satisfied with security infrastructure of the organisation. These participants viewed organisational well-being as theirs and protecting security was contributing to the organisational well-being in which each employee could play a significant role.

# 6 PRACTICAL IMPLICATIONS

From a managerial perspective, this study provided a starting point to organisations to reconsider current IT security programs. Understanding that compliance burnout caused by complying with security demands and active security engagement from receiving effective security resources can be the first step towards establishing an effective information security program.

First, it is important that organisations should introduce security compliance tasks in a new way that delivers simple, fun, interactive security instructions. Traditional method of developing written security policies needs to be reconsidered its effectiveness in promoting security compliance. . Second, security systems should be carefully reviewed to minimise impact on employees' work productivity and automate routine security tasks to reduce user involvement. Third, organisations should not rely on staff to spend extra effort in understanding and responding to standard security warnings. Instead risk information should be presented in illustrative and interactive formats where the users can easily assess the severity and relevance of the risks through visual analysis. Forth, organisations need to provide timely, responsive and effective technical security support.. Strict security controls may have counter-effect to security compliance as the users could become totally reliant and delegating to the IT department for security protection. Organisations should consider customising security controls for different groups of users to satisfy work needs and facilitates the ability to utilise and develop their skills. Last but not least, organisations should establish security compliance evaluation schemes that assess and recognise different levels of security compliance. Tangible or intangible rewards can be applied to recognise 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 organisation-wide culture which could have significant impact to individuals' compliance (Lacey 2010, Parsons et al. 2010).

# 7 CONCLUSION

The paper proposes a stress-based security compliance model that proposes system users may experience security compliance burnout from complying with security demands and engage with security activities as a result of receiving security resources. Compliance burnout and security engagement then affect the security compliance of the system users. Initial in-depth interviews with 17 users from three organisations identified three security demands and four organisationsal security resources that were considered important to encourage security compliance. Besides, the participants were found to expericence some levels of compliance burnout and security engagement in exercising security compliance at work.

Our initial findings establish a basis for further study to quantitatively examine the proposed stress-based security compliance model. The extent that security demands and security resources identified in this study affect security compliance should be assessed to strenghthen the initial model. This study also highlights the need to assess the burnout and engagement level in current security compliance programs.

## References


Bakker, A. B. & Demerouti, E. (2007). The Job Demands-Resources model: state of the art. Journal of Managerial Psychology, 22**,** 309-328.

Becker, G. S. (1968). Crime and punishment: an economic approach. Journal of Political Economy, 76.

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

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. Computers in Human Behavior, 28**,** 1849-1858.

Crawford, E. R., Lepine, J. A. & Rich, B. L. (2010). Linking job demands and resources to employee engagement and burnout: A theoretical extension and meta-analytic test. Journal of Applied Psychology, 95**,** 834-848.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hud, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. Computer & Security, 32**,** 90-101.

D'arcy, J., Herath, T. & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. Journal of Management Information Systems, 31**,** 285-318.

Demerouti, E., Bakker, A. B., Nachreiner, F. & Schaufeli, W. B. (2001). The job demands-resources model of burnout. Journal of Applied Psychology, 86**,** 499-512.

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

Dhillon, G. & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems, 16**,** 293-314.

Dwyer, D. J. & Ganster, D. C. (1991). The effects of job demands and control on employee attendance and satisfaction. JOURNAL OF ORGANIZATIONAL BEHAVIOR, 12**,** 595-608.

Fernet, C., Austin, S. P., Tre´Panier, S.-G. V. & 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, 22**,** 123-137.

Furnell, S. & Rajendran, A. (2012). Understanding the influences on information security behaviour. Computer Fraud & Security.

Guo, K. H. & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. Information & Management, 49**,** 320-326.

Herath, T. & Rao, H. (2009a). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18**,** 106-125.

Herath, T. & Rao, H. R. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47, 154-165.
Hovav, A. & D'arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. Information & Management, 49, 99-110.
Hu, Q., Xu, Z. C., Dinev, T. & Ling, H. (2011). Does Deterrence Work in Reducing information security Policy Abuse by employees? Communications of the ACM, 54, 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, 31, 83-95.
Kankanhalli, A., Teo, H.-H., Tan, B. C. Y. & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23, 139-154.
Lacey, D. (2010). Understanding and transforming organizational security culture. Information Management & Computer Security, 18, 4-13.
Lee, S. M., Lee, S.-G. & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41, 707-718.
Maddux, J. E. & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19, 469-479.
Padayachee, K. (2012). Taxonomy of compliant information security behavior. Computer & Security, 31, 673-680.
Pare, G. (2004). Investigating information systems with positivist case study research. Communications of the AIS, 13, 233-264.
Parsons, K., Mccormac, A., Butavicius, M. & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment. In: Defence, A. D. O. (ed.). Command, Control, Communications and Intelligence Division
DSTO Defence Science and Technology Organisation.
Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91, 93-114.
Saunders, M., Lewis, P. & Thornhill, A. (2012). Research methods for business students, Pearson Education.
Schaufeli, W. B. & Bakker, A. B. (2004). Job demands, job resources, and their relationship with burnout and engagement: a multi-sample study. Journal of Orgnizational Behavior, 25, 293-315.
Schaufeli, W. B., Leiter, M. P., Maslach, C. & Jackson, S. E. 1996. Maslach Burnout Inventory-General Survey. In: Maslach, C., Jackson, S. E. & Leiter, M. P. (eds.) The Maslach Burnout Inventory: Test manual. 3rd ed. Palo Alto, CA: Consulting Psychologists Press.
Schaufeli, W. B. & Taris, T. W. 2014. A critical review of job demands-resources model: Implications for improving work and health. In: Bauer, G. F. & Hammig, O. (eds.) Bridging Occupational, Organizational and Public Health: A Transdisciplinary Approach. Dordrecht: Springer Science+Business.
Vance, A. & Siponen, M. (2012). IS Security policy violations: A Rational choice perspective. Journal of Organizational and End User Computing, 24, 21-41.
Vance, A., Siponen, M. & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49, 190-198.
Yin, R. K. (2009). Case study research: Design and Methods, Thousand Oaks, CA: Sage.