Stress-Based IS Security Compliance: Towards a Conceptual Model

Hiep Cong-Pham
School of Business Information Technology and Logistics
RMIT University Vietnam
Ho Chi Minh City, Vietnam
Email: hiep.pham@rmit.edu.vn

Linda Brennan
School of Media & Communication
RMIT University
Melbourne, Victoria, Australia
Email: linda.brennan@rmit.edu.au

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

Abstract

This paper examines potential impacts of organisational factors on security compliance by applying the "work-stress model" of the Job Demands-Resources model to security behaviour. The paper proposes that IT users' compliance burnout and security engagement are results of coping with security demands and receiving resources respectively. Compliance burnout would reduce security compliance while security engagement would increase it. The security compliance model developed in this study emphasises developing emotional and cognitive resources from system users through effective provision of organisational resources and security requirements to promote desired security practice. Further assessment of the proposed model in this paper would extend behavioural security compliance research through employing a new organisational theory and enable organisations to focus on specific resources and design of security requirements that most encourage IT users' safe security behaviour.

Keywords Security compliance, compliance burnout, security engagement, security demands, security resources.

1 Introduction

The main objective of information security is to protect confidentiality, integrity and the availability of respective data, information and organisational computer services (Dhillon and Backhouse 2001). Protecting confidentiality is about ensuring that information can be accessible only by those who are authorised; information integrity measures protect the accuracy and completeness of information and processing methods, and information access and availability is about guaranteeing that authorised users have access to information and associated information resources (Dhillon and Backhouse 2001). For example, information confidentiality can be protected by authentication with username/password, data integrity with checksum and data verification, and availability with data and service backup, and authorisation techniques. In other words, information security is the practice of defending the safety of data and information in a computer system against unauthorised disclosure, modification, or destruction. Information security also protects the computer system itself and resources against unauthorised use, modification, or denial of service (von Solms and von Solms 2004).

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 training and communicate potential security risks to system users. Moreover, organisations can also enforce sanctions for security violations. Security training and security risk communications provide system users with necessary skills and knowledge to evaluate and respond to security threats (Furnell and Rajendran 2012a; Vance and Siponen 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).

Organisations develop security policies and procedures to require and guide employees to use available security resources and perform their responsibilities when dealing with information and computer resources. To fulfil these security responsibilities, which can vary in relation to the task volume and/or complexity, the users may need to acquire a certain level of computer and/or security knowledge and to spend time in applying security measures. Fulfilling expected security requirements can affect burnout if employees find performing security tasks to be time consuming, unclear, inconvenient and obstructing their daily work. Compliance burnout also occurs when security tasks require extra time, computer experience and/or security knowledge which the employees may not possess. For example, the need to maintain awareness of constantly changing cyber security risks, or learning complex security skills are security tasks that would impose a burden on employees in terms of time and cognitive effort. Finally, performing security tasks can add an extra workload on already stressed staff. Performing a high and/or frequent number of security measures requires IT users to spend extra time and handle workflow disruption while still being required to quickly respond to other work demands that can create anxiety, tension and make sustained mental attention difficult, thus reducing their security effort (Salanova et al. 2013).

The Job Demands-Resources model (JD-R) is a work stress model, which explains that employees' performance and well-being can be affected by both job demands and resources via the competing motivational processes of work burnout and engagement (Bakker and Demerouti 2007; Demerouti et al. 2001). Personal resources have been included in the extended JD-R model as a moderating factor between demands, resources, burnout and engagement that influence job performance, commitment and satisfaction (Bakker et al. 2010; Toner et al. 2012). 2- The JD-R model has been successfully adapted and studied for organisational performance aspects in some countries such as Spain, Greece, Italy, Norway, Sweden, Finland, Germany, Belgium, South Africa, China, and Australia (Bakker and Demerouti 2007).

The impact of compliance cost on safe security intention and behaviour has been inconsistently reported (Furnell and Rajendran 2012b; Ifinedo 2011; Vance et al. 2012). Few studies have examined how users develop cognitive and emotional stress due to continuing fulfilment of security demands (D'Arcy et al. 2014; Sommestad et al. 2014). There is a lack of information system literature that explores what aspects of security demands constitute negative or stressful compliance that can affect security behaviour as the nature of security tasks can cause stress and increase moral disengagement, which lead to security non-compliance (D'Arcy et al. 2014). Prior compliance studies have examined factors that influence users' involvement with security tasks, however, the energetic state or intrinsic motivation of such involvement, which is the security engagement, has not been investigated (Naudé and Rothmann 2006; Van Wyk et al. 2003). The concept of security engagement is drawn from work engagement, which has been identified as a critical source to motivate and maintain work commitment and performance in various contexts (Bakken and Torp 2012; Crawford et al. 2010).

Emboldening employees to become involved with security activities is important; nevertheless, the level of emotional and cognitive resources that people bring to performing security tasks might be a key to maintenance of expected security behaviour, even in an unfavourable security environment (Bakken and Torp 2012; Crawford et al. 2010). Given the JD-R model's significant relevance to security demands, resources, and the motivational processes of compliance burnout and engagement discussed in the previous section, the research question of this paper is constructed as follows.

- How do security demands, organisational and personal resources affect security compliance?

2 DEVELOPMENT OF A STRESS-BASED SECURITY COMPLIANCE CONCEPTUAL MODEL

The following section presents discussions of how stress and engagement in security compliance can affect users' security compliance in organisations.

2.1 Security Demands and Compliance Burnout

Security demands are security tasks and procedures that employees must perform as part of their responsibilities, such as accessing security policies for instructions and guidance, acquiring skills and knowledge to deal with changing security environments, and using security measures. Certain aspects of security requirements were demonstrated to negatively affect users' compliance. For example, the perceived cost of personal security responses has been proven to have different impacts on compliance intention and behaviour (Vance and Siponen 2012). People can view inconvenient, work hindering and time-consuming aspects of security tasks as a legitimate reason for not utilising a security measure (Bulgurcu et al. 2010). For example, an automated virus scan can disrupt an employee's intended work task because his or her computer slows down during the scan. Here the security task poses a work impediment to the employee. Work impediment of security tasks was reported to increase perceived cost of compliance (Bulgurcu et al. 2010) and negatively impact compliance intention (Vance and Siponen 2012). Complex and time-consuming security tasks such as use of security email was noticed to increase employees' stressful reactions (Puhakainen and Siponen 2010), or fast changing security environment contributed to internal security abuse (Posey et al. 2011).

The impact of stressful security demands on security behaviour can be assessed under the phenomenon of technology stress due to human cognitive limitations and inability to adapt to rapid advances in technology (Shu et al. 2011). Information overload, and uncertainty and complexity of information systems can lead to technology stress in IT users, which may negatively influence effective technology use and productivity (Salanova et al. 2013). Under technology stress, employees can feel negative affective experiences, such as exhaustion, scepticism and inefficacy towards the use of ICT, which then reduces professional commitment and effective use of the technology (Salanova et al. 2013). Technology stress is similar to compliance burnout in a security context where people can develop negative psychological states such as exhaustion and a distant attitude toward the use of security technologies at work.

Fulfilment of job demands can incur prolonged physical and psychological cost, eventually leading to work burnout - a negative psychological state (Demerouti et al. 2001). Work burnout is a main determinant of undesirable employee behaviour, such as low work productivity and deviance (Gilboa et al. 2008), negative job strain and impaired health (Demerouti et al. 2009), and psychological distress (Bruck et al. 2002). Adapting from the concepts of work burnout and technology stress, security compliance burnout reflects psychological exhaustion and cynicism toward complying with assigned security tasks and exercising security precautions. This research assumes that, due to the existence of high security demands and lack of resources, the employees experience an energy-draining process that results in fatigue and cynical views of security programs (Salanova et al. 2013; Schaufeli and Bakker 2004). Such negative psychological affective experiences would reduce cognitive attention and focus, as well as commitment in performing security compliance tasks.

The following hypothesis is proposed to explain the impact of security demands on compliance burnout.

- H1: Security demands are positively related to security compliance burnout

2.2 Organisational Security Resources, Security Compliance Burnout and Engagement

Job resources are those physical, social, or organisational aspects of the job that help facilitate achievement of work goals by reducing job demands' associated physical and psychological costs, and

promoting personal growth and development (Demerouti et al. 2001). Examples of job resources are performance feedback, job control, and financial rewards (Schaufeli and Taris 2014). The revised JD-R model incorporated the positive-psychological component namely work engagement as a result of receiving adequate job resources (Schaufeli and Bakker 2004).

Work engagement is considered as a motivational process that is created by job resources and mediates the impact of job demands and organisational commitment and performance (Schaufeli and Taris 2014). It is a persistent positive, fulfilling, work-related state of mind comprised of three psychological states: vigour, dedication, and absorption. Vigour represents the high level of energy and mental resilience in doing a task. Dedication is connected with enthusiasm, commitment, and persistence; and absorption means being focused and capable of effortless concentration, and intrinsic enjoyment. Engagement is also defined as an energetic state of performance in which the employee excels at performance at work and is confident of his or her effectiveness (Naudé and Rothmann 2006). Research on engagement has consistently demonstrated that it is associated with positive job attitudes (Schaufeli et al. 2008) and higher levels of performance at individual and unit levels (Salanova et al. 2005). Engagement in education has been acknowledged as a source of achievement and school behaviour across different levels of economic and social conditions (Handelsman et al. 2005), and resultant academic behavioural and social outcomes (Furrer et al. 2006). It is essential that people employ their physical, emotional and cognitive resources when they engage at work (May et al. 2004). Engagement can also be claimed to be a form of intrinsic motivation that comprises interest, enjoyment, and internal satisfaction in the regulatory process (Ryan and Deci 2000). In summary, work engagement includes elements of positive attitude toward the tasks, and energetic and mental resilience in performing them, which can be significant determinants of influencing security compliance intention and behaviour (Ryan and Deci 2000).

While security compliance can be defined as the task involvement, security engagement describes the extent of energy, enthusiasm, and enjoyment in performing security tasks. In other words, it is a form of intrinsic motivation or self-motivation in security compliance process where people take interest and enthusiasm in performing security tasks. Motivating people to perform security tasks can be a challenge where the more the employees are required to personally be involved in fulfilling the security tasks, the more resilient or less compliant they become (Adams and Sasse 1999). Security compliance burnout and engagement are often the results of experiencing an extended security practice under certain security environments. Performance of security demands, especially stressful ones, would require sustained focus and resilience from the employees. This research argues that people with higher security engagement would more be resilient, attentive to the security tasks and have a positive attitude toward complying with the policies, which should lead to better security compliance (Schaufeli and Bakker 2004). Security engagement to some extent is the direct opposite of compliance burnout. Energy and enthusiasm dimensions of security engagement are the opposites of exhaustion and cynicism dimensions of compliance burnout (Schaufeli and Bakker 2004). That means security engagement and burnout will have an opposite impact on security compliance, such that security engagement can lead to better compliance, while burnout would reduce it.

Similar to the role of job resources in the JD-R model, security resources could reduce security demands' associated physical and psychological costs, promote security engagement and achieve security goals (Demerouti et al. 2001). However, the JD-R model does not include certain resources that can mitigate the impact of demands on burnout or motivate engagement in a particular work context (Crawford et al. 2010; Schaufeli and Taris 2014). In terms of security management, it is the responsibility of the organisations to provide resources to facilitate their employees' completion of their security responsibilities. Depending on the nature of security demands, users may need different resources to comply properly.

Organisations' security supports often come in the forms of security awareness training, documentation on business applications and IT system (Ng et al. 2009), technical support (Ifinedo 2011; Vance et al. 2012) and financial rewards (Bulgurcu et al. 2010; Siponen et al. 2014). User training and system documentation can increase security-related awareness and provide adequate skills to cope with the complexity of the security tasks. Technical support also helps address users' IT and security-related problems and queries. A responsive and effective help desk can reduce work interruption, offset the effects of decreased productivity, and increase employees' satisfaction (Salanova et al. 2013). Financial rewards can be used to extrinsically motivate staff to perform security compliance as people weigh the benefits of doing the tasks (Vance and Siponen 2012). The effectiveness of rewards to increase compliance, however, is not yet clearly demonstrated in prior studies (Boss et al. 2009; Pahnila et al. 2007).

Security response efficacy is a factor to motivate employees to take protective measures against security threats (Vance et al. 2012). The resources and security measures that the organisations provide and implement to facilitate employees' security compliance do not only reduce an individual's IT effort but also demonstrate effectiveness of the security measures. Most security systems nowadays implement technical measures, such as automated antivirus systems, email spam prevention, network firewalls and automated user data backups. Automated technical measures can minimise involving users in security tasks and demonstrate the effectiveness of security measures. Users would be more likely to perform security activities when they understand the purposes of the security program, perceive security measures to be relevant and effective against risks, and are capable of fulfilling such tasks (Vance and Siponen 2012).

The effectiveness of security resources to assist users' compliance, however, can result in their reliance on the organisation for protecting information assets. For example, facilitating conditions, such as time to learn, easy access to security policies and support to comply, was shown to negatively influence attitudes towards compliance, contrary to the authors' original theory (Pahnila et al. 2007). An explanation can be that users consider security responsibilities should be dealt with by the organisation (Cox 2012). As a result, the more effective the security resources the more reliant on the organisation employees would be. Albrechtsen and Hovden (2009 explained that employees would leave complex security tasks to organisations and underestimated their roles in security protection.

Most studies on security compliance have not systematically examined which resources can be effective in reducing burnout and increasing engagement. For example, Parker et al. (2010) demonstrated higher self-determined employees experience greater engagement in the form of dedication to work if they are given higher job control, such as the ability to use skills or control the work practice. Identification of resources that may enhance security engagement can have an important practical implication. Organisations need to focus on providing the resources that could be effective in promoting employees' security compliance, not their reliance on the organisation for security protections.

To describe the impact of security resources on burnout and engagement, two hypotheses are developed as below.

- H2: Organisational security resources are negatively related to security compliance burnout
- H3: Organisational security resources are positively related to security engagement

2.3 Personal Resources, Security Compliance Burnout and Engagement

The original JD-R model mainly addresses the influence of work-related factors, namely, demands and resources on people's stress and job commitment without incorporating their personal resources (Schaufeli and Taris 2014; Xanthopoulou et al. 2007). Personal resources are mental and emotional self-competences that can affect how an individual appraises the work environment, copes and recovers from the stress process (Hobfoll et al. 2003). Self-efficacy can be regarded as one major personal resource. According to the Theory of Planned Behaviour (Ajzen 1991), perceived behavioural control (a form of self-efficacy) influences one's ability to mobilise motivation, cognitive resources, and emotional reactions, such as stress and anxiety, in response to a task. Xanthopoulou et al. (2007 observed that personal resources, such as self-efficacy, esteem, and optimism, mediated the impact of work demands and resources on employees' job performance. The authors argued that high-level self-efficacious employees would adapt better to a changing and challenging work environment, focus more on work resources than demands, hence experiencing higher level of engagement. The employees' resources can moderate the tension between work demands, resources and perceived burnout that influence individual job performance, commitment and satisfaction (Bakker et al. 2010; Toner et al. 2012). In regard to security behaviour, personal resources can be effective in coping with security demands and alleviating the negative impact of compliance burnout on compliance behaviour. They can also help users to take advantages of the resources and develop engagement with security activities.

As previously mentioned, security self-efficacy relates to a belief in an individual's capabilities to successfully perform their security tasks, as well as to cope with changing requirements. IT self-efficacy has been shown to affect anxiety related to ICT (Henderson et al. 1995), motivate continued computer use (Deng et al. 2004), and to help safeguard against burnout (Salanova 2000). An imbalance between a person's capabilities and the security demands can also create stress or burnout when there is an anticipation of negative consequences due to inadequate responses (Chen et al. Winter 2012-2013), or the requirements exceed one's capabilities and personal resources (Posey et al. 2011). Therefore, employees with high security self-efficacy would be willing to overcome the complexities of the security

tasks and cope with them more positively (i.e. engagement), decreasing the level of perceived compliance burnout (Shu et al. 2011).

Negative experience of security incidents could also influence one's confidence in one's self-efficacy. Exposure to security incidents, such as a virus infection, losing information, and online fraud causes a negative emotional state such as stress or anxiety, which could lower individuals' belief in their security self-efficacy (Rhee et al. 2009). Moreover, security exposure was shown to increase perceived benefits of compliance, perceived cost of non-compliance, and safety of resources to name a few, which then influenced overall assessments of consequences, security attitude, and eventually the intention to comply (Bulgurcu et al. 2010).

In summary, cognitive and emotional self-competences of personal resources can help individuals to buffer the impact of security demands on burnout and enable positive emotional responses towards security requirements, hence increasing security engagement. Self-efficacy and negative security experience can affect the security compliance process. Given the potential influence of personal resources on appraising burnout and exerting engagement in security behaviour, two hypotheses are put forward.

- H4: Personal resources are negatively related to security compliance burnout
- H5: Personal resources are positively related to security engagement

Finally, compliance burnout and engagement can oppositely affect users' complying with security policies and caution taking. Hence, the following hypotheses are constructed in pertaining to the effects of burnout and engagement on security compliance.

- H6: Security compliance burnout is negatively related to security compliance
- H7: Security engagement is positively related to security compliance

The conceptual research model of this study is depicted in Figure 1, which posits that security demands positively affect users' perceived compliance burnout (H1). While provision of organisational resources can reduce compliance burnout incurred by fulfilling security demands (H2), and develops security engagement (H3). Similarly, emotional and cognitive competences of users help alleviate burnout (H4) and boost engagement with security tasks (H5). Finally, compliance burnout, which causes psychological exhaustion and negative attitudes towards compliance, lowers the intention to comply (H6). In contrast, the energetic and enthusiastic level of participating in security programs increases security commitment and performance (H7).

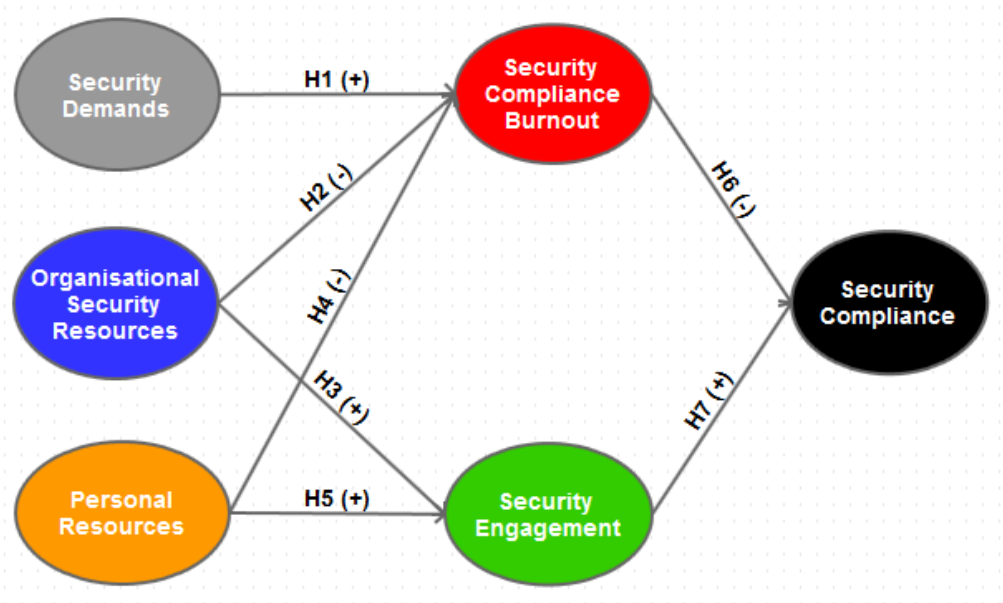

Figure 1: Stress-Based Security Compliance Conceptual Model

3 Conclusion and Future Work

Employees' unsafe security behaviour has been considered the weakest link in overall security programs. Security compliance with safe practice and guidelines is essential to minimise security risks caused by the users. Organisational and personal factors have been identified to influence security compliance whether facilitating or obstructing the compliance process. By employing a work-stress model, the JD-R model, to IS security context, the study hypothesised that security demands, organisational and personal factors can influence employees' security behaviour. Particularly, security tasks can be time-consuming and complex, provision of organisational resources may facilitate compliance and, at the same time result in employees' over reliance on the organisation for security protections, and users' IT competences which can all influence security behaviour. Moreover, two mediating factors of compliance burnout and engagement are also propositioned to explain the mechanism that security demands, organisational and personal resources impact on users' security compliance. First, security compliance burnout should mediate the influence of security demands on employees' complying with security policies. Security burnout can be reduced by receiving adequate organisational and personal resources. Second, security engagement is fostered by receiving organisational resources and can be further enhanced by individuals' own resources. Eventually, higher engagement with security activities should positively contribute to security compliance.

The study contributes to both theoretical and practical aspects. First, the paper explores the JD-R model to explain how combinations of organisational factors, including security demands, organisational and personal resources, such as, self-efficacy and security exposure, can influence security compliance. Motivational constructs from work stress literature such as burnout and engagement have been adapted in this paper to describe the impact of stressful security demands and provisions of adequate resources (organisational and personal) on security behaviour. Second, the expected findings from further assessment of the proposed model would provide useful insights to assist practitioners to develop effective security programs for organisations. Organisations need to be aware of users' burnout due to complying with security demands. Even though compliance burnout may not be fully avoidable, provision of effective resources can reduce the negative effect of compliance burnout on security behaviour.

The next stage of the study would be to conduct an empirical assessment of the conceptual model and enhance the explanatory power of the proposed model in various organisational contexts. In first phase, in-depth interviews with users and experts can be used to explore potential dimensions and correlations of the factors in the model. The findings from phase one would further refine the model which is then quantitatively tested using large scale surveys to establish significance and directional correlations of the identified factors.

4 References

Adams, A., and Sasse, M. A. 1999. "Users Are Not the Enemy," *Communications of the ACM* (42:12), pp. 40-46.

Ajzen, I. 1991. "Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Albrechtsen, E., and Hovden, J. 2009. "The Information Security Digital Divide between Information Security Managers and Users," *Computers & Security* (28:6), pp. 476–490.

Bakken, B., and Torp, S. 2012. "Work Engagement and Health among Industrial Workers," *Scandinavian Journal of Organizational Psychology* (4:1), pp. 4-20.

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* (15:7), pp. 622-636.

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

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

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* (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* (34:3), pp. 523-548.

Chen, Y., Ramamurthy, K., and Wen, K.-W. Winter 2012-2013. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *Journal of Management Information Systems* (29:3), pp. 157–188.

Cox, J. 2012. "Information Systems User Security: A Structured Model of the Knowing–Doing Gap," *Computers in Human Behavior* (28), 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* (95:5), pp. 834-848.

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

Demerouti, E., Bakker, A. B., Nachreiner, F., and Schaufeli, W. B. 2001. "The Job Demands-Resources Model of Burnout," *Journal of Applied Psychology* (86), 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* (14), pp. 50-68.

Deng, X., Doll, W., and Truong, D. 2004. "Computer Self-Efficacy in an Ongoing Use Context," *Behaviour & Information Technology* (23), pp. 395-412.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in Is Security Research: Towards Socio-Organizational Perspectives," *Information Systems* (11), pp. 127-153.

Furnell, S., and Rajendran, A. 2012a. "Understanding the Influences on Information Security Behaviour," *Computer Fraud & Security*:Feature Issue).

Furnell, S., and Rajendran, A. 2012b. "Understanding the Influences on Information Security Behaviour," *Computer Fraud & Security* (2012:3), pp. 12-15.

Furrer, C. J., Skinner, E., Marchand, G., and Kindermann, T. A. 2006. "Engagement Vs. Disaffection as Central Constructs in the Dynamics of Motivational Development," San Francisco, CA.

Gilboa, S., Shirom, A., Fried, Y., and Cooper, G. A. 2008. "Meta-Analysis of Work Demand Stressors and Job Performance: Examining Main and Moderating Effects," *Personnel Psychology* (61:2), pp. 227–271.

Guo, K. H., and Yuan, Y. 2012. "The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model," *Information & Management* (49), pp. 320-326.

Handelsman, M. M., Briggs, W. L., Sullivan, N., and Towler, A. 2005. "A Measure of College Student Course Engagement," *The journal of Educational Research* (98:3), pp. 184-191.

Henderson, R. D., Deane, F. P., and Ward, M. J. 1995. "Occupational Differences in Computer-Related Anxiety: Implications for the Implementation of Acomputerized Patient Management Information System," *Behaviour & Information Technology* (14), pp. 23–31.

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

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), pp. 83-95.

May, D. R., L., R., Harter, G., and Harter, L. M. 2004. "The Psychological Conditions of Meaningfulness, Safety and Availability and the Engagement of the Human Spirit at Work," *Journal of Occupational and Organizational Psychology* (77), pp. 22-37.

Naudé, J. L. P., and Rothmann, S. 2006. "Work-Related Well-Being of Emergency Workers in Gauteng," *South African Journal of Psychology* (36), pp. 63-81.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. C. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (4), pp. 815-825.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," in: *the 40th Hawaii International Conference on System Sciences*.

Parker, S. L., Jimmieson, N. L., and Amiot, C. E. 2010. "Self-Determination as a Moderator of Demands and Control: Implications for Employee Strain and Engagement," *Journal of Vocational Behavior* (76:1), pp. 52-67.

Posey, C., Bennett, R. J., Roberts, T. L., and Lowry, P. B. 2011. "When Computer Monitoring Backfires: Privacy Invasions and Organizational Injustice as Precursors to Computer Abuse," *Journal of Information Systems Security* (7:1), pp. 24–47.

Puhakainen, P. P., and Siponen, M. 2010. "Improving Employee' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757–778.

Rhee, H.-S., Kim, C., and Ryu, Y. U. 2009. "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior," *Computer & Security* (28), pp. 816-826.

Ryan, R., and Deci, E. 2000. "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions," *Contemporary Educational Psychology* (25), pp. 54-67.

Salanova, M., Agut, S., and Peiro´, J. M. 2005. "Linking Organizational Resources and Work Engagement to Employee Performance and Customer Loyalty: The Mediation of Service Climate," *Journal of Applied Psychology* (90), pp. 1217–1227.

Salanova, M., Grau, R. M., Cifre, E., &Llorens, S. 2000. "Computer Training, Frequency of Usage and Burnout: The Moderating Role of Computer Self- Efficacy," *Computers in Human Behavior* (16), pp. 575–590.

Salanova, M., Llorens, S., and Cifre, E. 2013. "The Dark Side of Technologies: Technostress among Users of Information and Communication Technologies," *International Journal of Psychology* (48:3), pp. 422-436.

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* (25), 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 *Bridging Occupational, Organizational and Public Health: A Transdisciplinary Approach,* G.F. Bauer and O. Hammig (eds.). Dordrecht: Springer Science+Business, pp. 43-67.

Schaufeli, W. B., Taris, T. W., and van Rhenen, W. 2008. "Workaholism, Burnout, and Work Engagement: Three of a Kind or Three Different Kinds of Employee Well-Being?," *Applied Psychology* (57), pp. 173–203.

Shu, Q., Tu, Q., and Wang, K. 2011. "The Impact of Computer Self-Efficacy and Technology Dependence on Computer-Related Technostress: A Social Cognitive Theory Perspective," *International Journal of Human-Computer Interaction* (27:10), pp. 923-939.

Siponen, M., Mahmood, M. A., and Pahnila, S. 2014. "Employee's Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51), pp. 217-224.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies," *Information Management & Computer Security* (22:1), pp. 42–75.

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* (52:5), pp. 637-642.

Van Wyk, R., Boshoff, A. B., and Cilliers, F. V. N. 2003. "The Prediction of Job Involvement for Pharmacists and Accountants," *SA Journal of Industrial Psychology* (29:3), pp. 61-67.

Vance, A., and Siponen, M. 2012. "Is Security Policy Violations: A Rational Choice Perspective," *Journal of Organizational and End User Computing* (24:1), pp. 21-41.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49), pp. 190-198.

von Solms, R., and von Solms, B. 2004. "From Policies to Culture," *Computer & Security* (23), pp. 275-279.

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* (14:2), pp. 121-141.

Copyright