Association for Information Systems
AIS Electronic Library (AISeL)

Research-in-Progress Papers | ECIS 2016 Proceedings

Summer 6-15-2016

SECURITY-RELATED STRESS – A NEGLECTED CONSTRUCT IN INFORMATION SYSTEMS STRESS LITERATURE

Clara Ament
Frankfurt University, ament@wiwi.uni-frankfurt.de

Steffi Haag
Frankfurt University, haag@wiwi.uni-frankfurt.de

SECURITY-RELATED STRESS – A NEGLECTED CONSTRUCT IN INFORMATION SYSTEMS STRESS LITERATURE

Research in Progress

Ament, Clara, Goethe University Frankfurt, Frankfurt, Germany, ament@wiwi.uni-frankfurt.de

Haag, Steffi, Goethe University Frankfurt, Frankfurt, Germany, haag@wiwi.uni-frankfurt.de

Abstract

Means of information security, such as security policies or security education, training, and awareness programs, are suggested to enhance employees' information security behavior. We posit that at the same time, exactly those security measures may have a negative effect, if employees perceive them, for instance, as difficult to understand, time-consuming, or an invasion of their privacy. However, focusing on pure technostress, information systems (IS) research so far has neglected stress induced by means of information security, although, there is first insight on the relevance of security-related stress for IS management.

Therefore, in this research-in-progress, we employ the person-environment (PE) fit model to build on as well as expand the existing IS stress literature. We thereby develop a first comprehensive framework of security-related stress, which considers non-technological aspects of security-related stress of employees' work, personal, and social environment. In doing so, we propose a multidimensional second-order construct and conceptualize how security-related stress affects employees' productivity directly and indirectly by promoting their perceived level of technostress. The results of our study should help IS management to anticipate and consider the downfalls of information security requirements when formulating companies' information security measurements, and thus limit the "dark side" of information security.

Keywords: Security-Related Stress, Technostress, Behavioral Information Security, Productivity.

1 Introduction

Until recently, research has focused on the technical side of information security, thereby omitting the user. Today, however, companies see their employees as the most frequent source of security threats (PwC, 2015). Staff, for instance, by using weak passwords, ignoring updates, sending sensitive data without encryption, unintentionally or deliberately provoke security breaches (Guo, 2013; Willison and Warkentin, 2013). Such employee behavior leads to complex problems for information systems (IS) management, for example in terms of value creation, if competitors get a hold of data on research and development, or competitiveness, if a company dealing with sensitive customer data in consequence of a security flaw loses customers' trust. To address, among others, the threat from the inside, organizations have increased their security investments (PwC, 2015).

Behavioral information security suggests various means such as information security policies as well as security education, training, and awareness programs, referred to as SETA programs (D'Arcy et al., 2009; Whitman, 2003). Those measures have the purpose to decrease, at best eliminate, human security shortcomings. Optimally, personnel is equipped with a sound security orientation or security decision making is even taken completely from staff. Though, violations of information security policy still occur and remain troublesome for businesses. One reason for this ineffectiveness of

behavioral information security techniques is the psyche of employees, more precisely, the stress employees are confronted with when facing information security-related requirements. Research has shown that stressful information security requirements, which are supposed to enhance the information security behavior of the workforce, actually induce the opposite effect. Such requirements may impose stress on employees, as they are, for instance, time-consuming, difficult to understand, or seen as a privacy invasion (D'Arcy et al., 2014b).

Technostress, which emerges when being confronted or working with new technologies, has been increasingly examined by IS research (Ayyagari et al., 2011; Ragu-Nathan et al., 2008; Tarafdar et al., 2010). Nevertheless, D'Arcy et al. (2014a) call for more substantial work regarding technostress, including the theoretical development across varying domains and in differing contexts. For example, while focusing on technostress, IS research has neglected further causes of stress related to IS usage, such as stress induced by information security instructions (D'Arcy et al., 2014b).

Hence, one of those fields promising to contribute to technostress research is information security. In this study, we therefore extend the extant knowledge on technostress by considering stress employees are confronted with when facing information security issues. We build on the person-environment (PE) fit model (Cooper et al., 2001; French et al., 1982) and develop a comprehensive construct of security-related stress, thereby considering non-technological aspects of security-related stress of employees' work, personal, and social environment. Results of our study should help IS management to anticipate and consider the downfalls of information security requirements when formulating companies' information security measures, and thus limit the "dark side" of information security (D'Arcy et al., 2014a). The structure of this research-in-progress is as follows: First we review previous IS stress research. Subsequently, we conceptually develop a model of stressors evoked by information security challenges as well as requirements and hypothesize their effect on employees' productivity. We end with a discussion of our future research endeavor.

2 Related Work

To build up a foundation for our conceptional model of stress resulting from information security measures, in this section, we give a brief introduction on prior IS stress research. IS stress research has focused almost exclusively on technostress, but recently a first attempt of discussing stress linked to behavioral information security requirements has emerged.

2.1 Technostress

Technostress results from the integration of information and communication technology (ICT) into daily life and can be described as an "inability to cope with the new technologies in a healthy manner" (Brod, 1984). Tarafdar et al. (2005; 2007) are the first to explore technostress from an IS perspective. They develop a model investigating the impact of technostress on individual productivity as well as role stress, which they validate by means of a survey. In the course of this, they identify five technostress creators, listed and explained in the following.

- Techno-complexity: Employees have to invest time and effort to understand and learn how to work with new technologies. Thereby, confusion results from jargon, multiplicity of functions, etc.
- Techno-insecurity: The pressure of job loss to a person with a better understanding of new IS features is ubiquitous for employees.
- Techno-invasion: Employees are always connected, which is why they can be contacted independent of place or time. Consequently, their working life overlaps with their personal life.
- Techno-overload: Employees have to accomplish more work in less time and are confronted with more input than they can handle or use. Furthermore, this involves interruptions and multitasking.

- Techno-uncertainty: An infinite technology transition prevents employees from developing an experiential basis. They have to regularly refresh their knowledge.

Building on this, Tarafdar et al. (2010) identify user involvement in the development of technology tools as well as support mechanisms for innovation as means to mitigate the negative effect of technostress. Later they adjust technostress inhibitors to a four-factor structure (Tarafdar et al., 2011). Ragu-Nathan et al. (2008) find technostress creators to have an inverse effect on employees' job satisfaction and, thus, indirectly decreasing commitment. On the other side, technostress inhibitors are found to have a positive direct effect on both variables. Furthermore, these studies shed light on the effect of user demographics on technostress. Srivastava et al. (2015) reveals how different personality types experience and deal with technostress. Job burnout and engagement, as two possible job outcomes, are studied. As stress is context-specific, Tarafdar et al. (2015) examine technostress from the perspective of a professional salesperson. Among other effects, they prove a positive relationship between technology self-efficacy and sales performance. Utilizing the PE fit model, Ayyagari et al. (2011) shed light on the individual importance of technology characteristics concerning technostress. Hung et al. (2011) explore "ubiquitous technostress", which is stress caused by excessive use of mobile technologies. Their research reveals a negative effect of ubiquitous technostress creators and a reverse effect of ubiquitous technostress inhibitors on productivity.

Contrary to the survey-based measurement approaches of the above mentioned studies, Galluch et al. (2015), Riedl (2013), and Riedl et al. (2012) rely on neurobiological experiments to measure, for instance, the level human stress hormones. Galluch et al. (2015) discloses the significance of different ICT-enabled control mechanisms, namely timing, method, and resource control, on episodic stress from ICT-enabled interruptions.

2.2 Security-Related Stress

Despite its steadily increasing scope, technostress research has only recently embraced the field of behavioral information security. To the best of our knowledge D'Arcy et al. (2014b) is the only work focusing on stress in the this context. Based on coping and moral disengagement theory, the study explores stress due to information security requirements, referred to as security-related stress, and its relationship to intentional violations of information security policies. Drawing on former work on technostress, they explore a three-dimensional view of security-related stress. Survey results confirm that stress from information security requirements increases moral disengagement and, in turn, security policy violations. The three attributes of security-related stress are stated and described below.

- Security-related complexity: Confusion results from a variety of contingencies, jargon, and other aspects of security. Employees have to invest time and effort to understand and apply measures of information security.
- Security-related overload: Information security requirements increase the employees' workload. Therefore, they have to accomplish more work in less time.
- Security-related uncertainty: Employees are confronted with continuous changes regarding information security requirements, preventing the development of an experiential information security basis. Hence, they have to regularly refresh their information security knowledge.

In summary, research on stress induced by information security has been neglected, while there is first evidence of its relevance for significant organizational outcomes. To address this gap and provide more insights into the topic, including non-technological aspects, we develop a comprehensive construct of security-related stress and model how security-related stress emerges and influences performance. Thereby, we build upon D'Arcy et al. (2014b) as well as the technostress literature, which has been outlined above.

3 Theoretical Framework and Hypothesis Development

In this section we develop our individual-level model of security-related stress and derive respective hypotheses. We employ the PE fit model as a theoretical lens, which follows the premise that an equilibrium relationship between people and their environment exists, leading to stress if this relationship is unbalanced (Cooper et al. 2001; French et al., 1982). In doing so, we adapt and extend prior technostress research, in particular the model of Tarafdar et al. (2005; 2007; 2010), by conceptualizing how measures of behavioral information security provoke stress in employees, which in turn affects their productivity directly as well as indirectly by enhancing their evaluation of technostress, i.e., stress related to technology itself. Employees' productivity is chosen as dependent variable as it is a key outcome variable in technostress research with a likewise relevance for organizations in practice (Hung et al., 2011; Tarafdar et al., 2005; 2007; 2010). Building on this work, we define productivity as "an individual's ability to effectively accomplish his or her tasks" (Tarafdar et al., 2007). Figure 1 depicts the suggested research model.

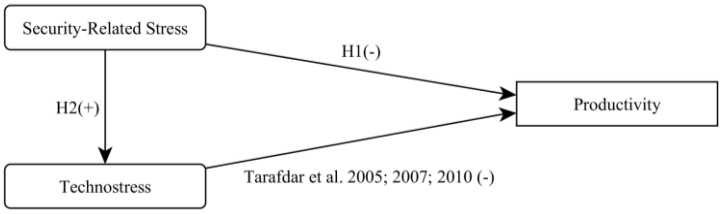

Figure 1. The impact of security-related stress on technostress and productivity

3.1 Security-Related Stress and Its Effect on Productivity

Information security measures supply employees with an orientation for security-related decisions. We posit that at the same time, they cause security-related stress, as a person's values or abilities are not in line with individual environmental demands or supplies, as stated in the PE fit model, (Cooper et al., 2001; French et al., 1982). Figure 2 depicts our multidimensional construct of security-related stress and its sub-dimensions. Existing dimensions derived from technostress research are highlighted in gray. Although we maintained their original denomination for pragmatic reasons, we adapted their content to our context of information security. In addition, we enhanced past work and added three further dimensions, which our literature review and expert discussions identified to be important and specific for security-related stress. To get a good overview of the resulting dimensions, we classify the sub-constructs into three different categories. Accordingly, creators of security-related stress are considered in categories of work, personal, and social environment.

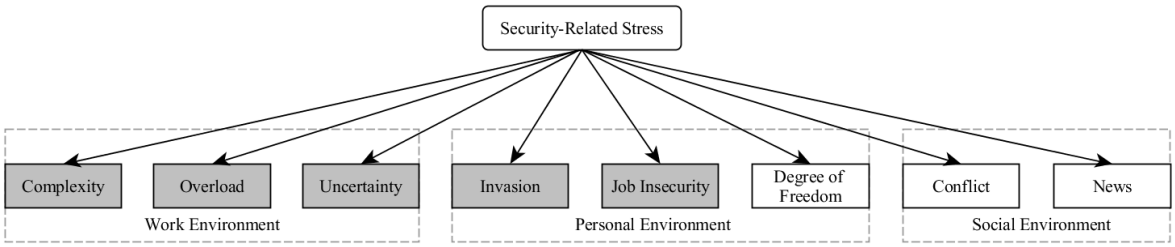

Figure 2. Multidimensional construct of security-related stress

In line with past research on technostress, we discuss security-related stress as multidimensional second-order construct consisting of conceptually distinct, but interrelated manifestations. The multidimensional measurement enables the development of a complex theoretical concept with relatively simple abstractions (Wright et al., 2012). Thus, this approach is consistent with our goal to

analyze the impact of varying creators of security-related stress on employee's perceived technostress and productivity. In the following three subsections, we introduce the different categories and the respective creators of security-related stress and hypothesize their impact on employees' productivity.

3.1.1 Security-Related Stress Regarding Employees' Work Environment

Employees may encounter security-related stress as to their work environment in terms of complexity, overload, and uncertainty. Those technostress creators have been originally introduced by Tarafdar et al. (2005, 2007). D'Arcy et al. (2014b) transfer them to their construct of security-related stress.

Having to deal with information security increases job demands towards employees (Albrechtsen and Hovden, 2009) by imposing additional ever-changing requirements. Employees might be obliged to spend time and effort on learning, understanding, and implementing those security requirements. However, the complexity of security requirements may exceed a person's intellectual abilities, leading to problems of understanding or misunderstanding of security policies. For instance, a consultant, who works at a client, is not able to understand what a safe connection to a company's intranet is and how to build up such a connection. Hence, his performance should decline, as he has to acquire this knowledge before being able to work effectively.

In addition to assigned tasks, staff has to cope with information security. Consequently, employees, due to overload, could be forced to work longer or faster. A high workload from information security leads to a conflict of interest between functionality and security (Albrechtsen, 2007). Especially, the application of security controls pressurizes employees, as they believe they have to keep the same performance level they had before security requirements were introduced (Posey et al., 2011). Furthermore, the introduction of new security requirements may interrupt the habitual work flow of employees and distract them, thus stressing them. One example of such a distraction is a security window that interrupts the workflow and forces a decision from the employee. An example of security overload is having to use and remember a variety of different passwords, which comply with the company's security standards. As a consequence of overload employees' productivity should drop.

Another creator of security-related stress might be uncertainty. As technology constantly develops, and new updates arise to existing tools, new security issues appear and in reaction to these new security requirements. In this context, employees might not have enough time to build up a solid security routine. Along, they have to continually refresh their security knowledge. Hence, frequent changes in tasks with respect to information security demands should lead to stress among the workforce and lower the employees' productivity.

3.1.2 Security-Related Stress Regarding Employees' Personal Environment

Besides job complexity, overload, and uncertainty, job insecurity and privacy invasion are recognized as creators of technostress. In contrast to D'Arcy et al. (2014b), we include them in our construct of security-related stress because research points to their existence also in the security context (Young, 2010). Along with the dimension degree of freedom, they form the category of security-related stress as to employees' personal environment. Those dimensions of security-related stress relate to individual attributes including personal goals and motivation, as well as self-efficacy.

Frequently, individuals are confronted with situations of high security relevance, which are neither covered by the security policy, nor have been subject of their security training. An employee has to invest extra time contacting his principal or, if available, a security officer, as wrong decisions could lead to severe security incidents. Moreover, employees might be left in charge of security decisions. Especially, for employees with low self-efficacy, responsibility may result in stress (Matsui and Onglatco, 1992), as they question their own abilities and have to bear their decisions' consequences, as well. Having to invest extra time to self-responsibly take a security decision or asking for advice could limit the productivity of employees. By contrast, due to the requirements of information security, staff could also feel restricted in its freedom. Employees have to change their habits and way of working

when including security procedures in their workflow. This can trigger stress and might lead to a fall in productivity, as employees have to customize. Restrictions may leave limited room for autonomy, and, thus, as innovative thinking declines, in the long-run productivity might be reduced. This coincides with the insight on innovation from Tarafdar et al. (2010).

Moreover, information security requirements can be a source of job insecurity among the workforce. During the assessment of their work, employees may not be solely evaluated in terms of quality and quantity of their task-fulfillment, but their assessment could likewise depend on security adherence. An employee who performs excellent, but caused a consequential breach of security might even face job loss (Young, 2010). Thus, the anxiety to fulfill an assignment according to expectations should rise, leading to stress. As one possible reaction to deal with this anxiety, employees might focus more strongly on matters of information security, thereby reducing the effort invested in accomplishing their actual tasks. Consequently, productivity would decline.

Besides, measures of information security may invade the personal lifes of employees. For example, due to security precautions, some firms ask their staff to hand in all personal devices when entering company buildings, not handing them back until the employees leave the building again. Similar is true for the electronic monitoring of employees (Aiello and Kolb, 1995; Smith et al., 1992) concerning, for instance, their Internet usage. Employees might understand such security measures as an invasion of their privacy. As a consequence, means of information security can even lead to an increase in computer abuse intention (Posey et al., 2011), thus, being counterproductive.

3.1.3 Security-Related Stress Regarding Employees' Social Environment

Social security-related stress refers to stress individuals suffer as they interact with other persons. This sub-dimension exclusively considers non-technological aspects of security-related stress. Creators of social security-related stress include conflict and news.

Conflicts are frequently stated as one of the most common stressors at the workplace (Ongori and Agolla, 2008). Conflicts might, for instance, arise when the instructions of supervisors are not in line with established information security requirements. In such situations employees would be exposed to stress as they have to decide whether to confront the superior with the noncompliance or to violate existing regulations. A similar conflict may arise due to group pressure. For example, if security policies stated that computer passwords must not be shared, an employee, who will be on leave, could refuse to give his computer password to a colleague, who is supposed to be his vacation replacement. This colleague may argument it being common practice among colleagues and important for facilitating his work. Confronted with this situation, the leaving employee might feel stressed. Such conflicts limit productivity of employees (Dreu and Weingart, 2003) as they have to spend some of their resources on solving conflicts. Going back to the example, the time the employee would spend on arguing with his colleague, reflecting on the situation, and finding a proper solution, which is in line with security requirements, cannot be used on his assigned tasks, resulting in lower productivity.

News on major security gaps in utilized software or reports on substantial security breaches leading to the misuse of sensitive data could be seen as another source of social security-related stress. This coincides with the theory on fear appeals describing the impact of persuasive messages, which include the element of threat, on end user behavioral intentions (Johnston and Warkentin, 2010). On the one hand, news may improve the awareness of information security among staff. However, employees could become overcautious and spend an excessive effort on security measures. On the other hand, news could frighten employees and limit their use of IS. Thus, the positive enabling effect of technology would vanish, and productivity would decrease. To conclude and build on our discussion about the impact of each security-related stress manifestation on productivity, we hypothesize a negative effect of security-related stress on the individual productivity of employees.

Hypothesis 1: Security-related stress is negatively associated to individual productivity.

3.2 Effect of Security-Related Stress on Technostress

After analyzing sources of stress due to information security, we now turn to our second hypothesis and argue on the promoting effect security measures have on technostress. Therefore, we separately investigate the effect of security-related stress as a holistic construct on the individual creators of technostress. Each creator represents one manifestation of the multidimensional construct of technostress, introduced by Tarafdar et al. (2005; 2007).

In terms of complexity, employees have to first understand technology and tools before being able to use and reasonably integrate them into their work processes. Therefore, additional information security requirements may add to the complexity of technology and tools. The already elaborate learning process might become even more troublesome. For instance, if writing an email instead of a letter is already putting an excessive demand on an employee, having to encrypt this email before sending might be perceived as an additional challenge. Thus, stress due to information security should have a positive effect on techno-complexity.

Insecurity, with respect to technostress describes the pressure IS users feel regarding job loss. Information security measures most likely will strengthen this fear, as they demand additional knowledge from staff. They might undergo a constant fear of losing their job to a person with better IS qualifications including information security. To strengthen their position, it is conceivable that employees keep back security relevant information from potential competitors. Overall this suggests a rise of stress from technology insecurity due to security-related stress.

As introduced above, invasion resembles stress from being permanently connected. If the usage of ICT from outside the office is subject to additional security rules, technostress might increase due to security-related stress. For instance, many firms request their staff to take security precautions, such as the use of security tokens or virtual private networks, when accessing their emails from outside the office. Hence, work life further invades private life. In the case that security compliance is monitored during off-hours, employees might fear giving away personal matters, thus causing additional stress. Consequently, security-related stress should positively affect perceived technostress. It is arguable that employees, who do not have to work off the job, could feel a stress relief as messages are not pushed to their phones. However, their technostress base level should be minor, as well.

The usage of technology tools should lead to an input overload among staff making use of those tools. Employees are forced to extend their working time or speed up their working pace. Means of security run up the information, tasks, and rules employees are confronted with. Accordingly, they would have to work even faster or further extend their working hours. Thus, technostress from overload should increase due to security-related stress. Furthermore, even if there are applications, like a junk mail filter that ease technostress as it takes away some of the mass of information, most security tools, such as virus scanners, may interrupt the work flow or worsen multitasking.

Security-related uncertainty stresses employees, because they have to regularly update their knowledge on technologies and tools. Security actions usually are reactions to arising loopholes in technologies. Frequently, when new technologies become available, not all security consequences are foreseeable, potentially leaving security decisions to staff. Having to make such decisions can result in stress. Consequently, security requirements should reinforce the stress due to techno-uncertainty.

Overall, we therefore posit that if employees already suffer from stress when dealing with new technologies or tools, this stress will even increase when being confronted with security measures. Accordingly, we hypothesize that security-related stress has a positive effect on technostress.

Hypothesis 2: Security-related stress is positively associated to technostress.

4 Contribution and Future Research

To advance our understanding of the prevalent lack of security measures' efficacy, in this study, we suggest security-related stress as one cause of those shortcomings. To the best of our knowledge, this paper is the very first developing a comprehensive framework of security-related stress, including non-technological facets, thereby shedding light on the relationship between stress from information security and technostress as well as their effect on productivity. Building on and extending technostress literature, we discuss creators of security-related stress spanning an employees' work, personal, and social environment. Furthermore, we hypothesize a positive effect of security-related stress on employees' technostress and a negative effect on their productivity.

Gaining further insights on security-related stress is of great interest to IS management. Based on our study, practitioners can anticipate and consider the downfalls of information security measures when formulating companies' security policies, including regulations as well as SETA programs, thus enhance their effectiveness and limit the "dark side" of information security. Ultimately, employees benefit from this research when working and living in an environment tailored to their needs.

We are still right at the beginning of investigating security-related stress. Thus, this research-in-progress is a first deep dive into the subject. Our next steps will include item development based on transferring and adapting available scales of the introduced related work (e.g., Ayygari et al., 2011; D'Arcy et al., 2014b; Nagu-Rathan et al., 2008; or Tarafdar et al., 2010) to our research context as well as developing new scales. Therefore, we plan to discuss each item with industry experts and experienced IS researchers first and pretest the scales in a preliminary survey.

In addition to security-related stress, the questionnaire-based data collection will capture closely related constructs, such as self-efficacy or innovativeness, and demographic variables because security-related stress may, for instance, vary across industries. After a pretest, the survey, to ensure a homogeneous group of participants, will be distributed among employees working in the hotel industry. For this industry, information security plays a role of upper importance. Workforce, which undergoes strong fluctuations and working hours around the clock, gets in touch with sensitive customer data. Shortcomings, such as the release of guests' credit card numbers, lead to a severe loss of confidence among customers and the violation of regulatory credit card standards. Therefore, the secure handling of these data must be ensured at any time.

References

Aiello, J.R. and Kolb, K.J. (1995), "Electronic Performance Monitoring and Social Context: Impact on Productivity and Stress", *Journal of Applied Psychology*, Vol. 80 No. 3, pp. 339–353.

Albrechtsen, E. (2007), "A Qualitative Study of Users' View on Information Security", *Computers & Security*, Vol. 26 No. 4, pp. 276–289.

Albrechtsen, E. and Hovden, J. (2009), "The Information Security Digital Divide between Information Security Managers and Users", *Computers & Security*, Vol. 28 No. 6, pp. 476–490.

Ayyagari, R., Grover, V. and Purvis, R. (2011), "Technostress: Technological Antecedents and Implications", *MIS Quarterly*, Vol. 35 No. 4, pp. 831–858.

Brod, C. (1984), *Technostress: The Human Cost of the Computer Revolution*, Reading, MA, USA: Addison Wesley Publishing Company.

Cooper, C.L., Dewe, P.J. and O'Driscoll, M.P. (2001), *Organizational stress: A review and critique of theory, research, and applications*, Los Angeles: Sage.

D'Arcy, J., Gupta, A., Tarafdar, M. and Turel, O. (2014a), "Reflecting on the "Dark Side" of Information Technology Use", *Communications of the Association for Information Systems*, Vol. 35 No. 1, pp. 109–118.

D'Arcy, J., Herath, T. and Shoss, M.K. (2014b), "Understanding Employee Responses to Stressful Information Security Requirements. A Coping Perspective", *Journal of Management Information Systems*, Vol. 31 No. 2, pp. 285–318.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse. A Deterrence Approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79–98.

Dreu, C. and Weingart, L. (2003), "Task versus Relationship Conflict, Team Performance, and Team Member Satisfaction. A Meta-Analysis", *Journal of Applied Psychology*, Vol. 88 No. 4, pp. 741–749.

French, J.R.P., Jr., Caplan, R.D. and Harrison, R.V. (1982), *The mechanisms of job stress and strain*, London: Wiley.

Galluch, P.S., Grover, V. and Thatcher, J.B. (2015), "Interrupting the Workplace: Examining Stressors in an Information Technology Context", *Journal of the Association for Information Systems*, Vol. 16 No. 1, pp. 1–47.

Guo, K.H. (2013), "Security-related Behavior in Using Information Systems in the Workplace. A Review and Synthesis", *Computers & Security*, Vol. 32, pp. 242–251.

Hung, W.-H., Chang, L.-M. and Lin, C.-H. (2011), "Managing the Risk of Overusing Mobile Phones in the Working Environment: a Study of Ubiquitous Technostress", In: *Proceedings of the 15th Pacific Asia Conference on Information Systems*, Brisbane, p. 81.

Johnston, A.C. and Warkentin, M. (2010), "Fear Appeals and Information Security Behaviors: An Empirical Study", *MIS Quarterly*, Vol. 34 No. 3, pp. 549–566.

Matsui, T. and Onglatco, M.-L. (1992), "Career Self-Efficacy as a Moderator of the Relation between Occupational Stress and Strain", *Journal of Vocational Behavior*, Vol. 41 No. 1, pp. 79–88.

Ongori, H. and Agolla, J.E. (2008), "Occupational Stress in Organizations and Its Effects on Organizational Performance", *Journal of Management Research*, Vol. 8 No. 3, pp. 123–135.

Posey, C., Bennett, B., Roberts, T. and Lowry, P.B. (2011), "When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse", *Journal of Information System Security*, Vol. 7 No. 1, pp. 24–47.

PwC (2015), *Turnaround and Transformation: Key Findings from the Global State of Information Security Survey 2016*, available at: www.pwc.com/gsiss (visited on 10/30/2015).

Ragu-Nathan, T.S., Tarafdar, M., Ragu-Nathan, B.S. and Tu, Q. (2008), "The Consequences of Technostress for End Users in Organizations. Conceptual Development and Empirical Validation", *Information Systems Research*, Vol. 19 No. 4, pp. 417–433.

Riedl, R. (2013), "On the Biology of Technostress: Literature Review and Research Agenda", *ACM SIGMIS Database*, Vol. 44 No. 1, pp. 18–55.

Riedl, R., Kindermann, H., Auinger, A. and Javor, A. (2012), "Technostress from a Neurobiological Perspective", *Business & Information Systems Engineering*, Vol. 4 No. 2, pp. 61–69.

Smith, M.J., Carayon, P., Sanders, K.J., Lim, S.-Y. and LeGrande, D. (1992), "Employee Stress and Health Complaints in Jobs with and without Electronic Performance Monitoring", *Applied Ergonomics*, Vol. 23 No. 1, pp. 17–27.

Srivastava, S.C., Chandra, S. and Shirish, A. (2015), "Technostress Creators and Job Outcomes. Theorising the Moderating Influence of Personality Traits", *Information Systems Journal*, Vol. 25 No. 4, pp. 355–401.

Tarafdar, M., Ragu-Nathan, B., Ragu-Nathan, T. and Tu, Q. (2005), "Exploring the Impact of Technostress on Productivity" In: *Proceedings of the 36th Annual Meeting of the Decision Sciences Institute*, San Francisco, p. 13771-13776.

Tarafdar, M., Tu, Q., Ragu-Nathan, B.S. and Ragu-Nathan, T.S. (2007), "The Impact of Technostress on Role Stress and Productivity", *Journal of Management Information Systems*, Vol. 24 No. 1, pp. 301–328.

Tarafdar, M., Tu, Q. and Ragu-Nathan, T.S. (2010), "Impact of Technostress on End-User Satisfaction and Performance", *Journal of Management Information Systems*, Vol. 27 No. 3, pp. 303–334.

Tarafdar, M., Tu, Q., Ragu-Nathan, T.S. and Ragu-Nathan, B.S. (2011), "Crossing to the Dark Side: Examining Creators, Outcomes, and Inhibitors of Technostress", *Communications of the ACM*, Vol. 54 No. 9, p. 113.

Tu, Q., Wang, K. and Shu, Q. (2005), "Computer-related Technostress in China", *Communications of the ACM*, Vol. 48 No. 4, p. 77.

Weil, M.M. and Rosen, L.D. (1997), *Technostress: Coping with Technology @Work @Home @Play*, Etobicoke, ON, Canada: John Wiley & Sons.

Whitman, M.E. (2003), "Enemy at the Gate: Threats to Information Security", *Communications of the ACM*, Vol. 46 No. 8, pp. 91–95.

Willison, R. and Warkentin, M. (2013), "Beyond Deterrence: An Expanded View of Employee Computer Abuse", *MIS Quarterly*, Vol. 37 No. 1, pp. 1–20.

Wright, R.T., Campbell, D.E., Thatcher, J.B. and Roberts, N. (2012), "Operationalizing Multidimensional Constructs in Structural Equation Modeling: Recommendations for IS Research", *Communications of the Association for Information Systems*, Vol. 30 No. 1, pp. 367–412.

Young, K. (2010), "Policies and Procedures to Manage Employee Internet Abuse", *Computers in Human Behavior*, Vol. 26 No. 6, pp. 1467–1471.