How Information Security Requirements Stress Employees

Completed Research Paper

Clara Ament
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4
60323 Frankfurt am Main
Germany
ament@wiwi.uni-frankfurt.de

Steffi Haag
Technische Universität Darmstadt
Hochschulstraße 1
64289 Darmstadt
Germany
haag@ise.tu-darmstadt.de

Abstract

To increase information security awareness among their workforce and to achieve secure information systems (IS), decision-makers employ measures of information security, such as security policies or associated training and educational programs. However, these information security measures might also put stress on employees, so-called security-related stress, for instance, if they are perceived as difficult to understand, as an invasion of privacy, or if they give rise to conflicts of interest.

While previous IS security research directly applies the existing concept of technostress to the security context, we develop and validate a more specific and holistic construct of security-related stress manifested in multidimensional stressors of individuals' work, personal, and social environment. A first empirical test with 165 participants does not only confirm the newly identified sub-dimensions, but also shows mixed effects of the interrelated but distinct sub-dimensions of security-related stress on information security policy compliance intention.

Keywords: Security-related stress, IS security, ISP compliance intention, technostress

Introduction

Over the last years, the frequency of information security incidents, such as intellectual property or customer data theft, has increased tremendously and along with these the financial loss affected organizations are confronted with (Ponemon Institute 2015; PWC 2015). Often overlooked negative long-term effects, such as damages to reputation or a decline in customer trust, top off the fatal effects information security incidents can have on businesses.

Frequently, such incidents originate from the unaware or aware but non-malicious behavior of organization's own employees (Guo 2013). To overcome this issue, research on behavioral information security has suggested various approaches covering, among others, information security policies (Bulgurcu et al. 2010), awareness programs (Tsohou et al. 2013), and trainings (Puhakainen and Siponen 2010). Such measures are supposed to decrease shortcomings in employees' security behavior and equip personnel with a sound orientation for security decision-making.

However, secure information systems (IS) will not be achieved if employees perceive elements of behavioral information security or even a company's entire information security strategy as difficult to understand, overwhelming, or time-consuming (D'Arcy et al. 2014). Similar is true if people sense an invasion of their privacy arising from the information security measures (Lee et al. 2016). In other words, employees can feel stressed due to organizational information security requirements and experience so-called security-related stress which can negatively affect information security policy (ISP) compliance (D'Arcy et al. 2014). While

the scarce previous studies on security-related stress adopt the concept of technostress, i.e., stress which results from the inability to cope with new technologies (Brod 1984), and transfer its sub-dimensions straightforward to the context of information security, this study also considers additional dimensions specific to the security-related context. First evidence from research and practice points to the relevance of stress in terms of individuals' work, personal, and social environment (Albrechtsen and Hovden 2009; Ament and Haag 2016; Young 2010). Building on this, we follow established approaches (MacKenzie et al. 2011) and develop a multidimensional construct of security-related stress. To empirically validate the multidimensional nature of the security-related stress construct, a pilot study is conducted among 165 employees of different companies varying in size and industry. The results do not only confirm the multiple dimensions of the security-related stress construct but also emphasize the importance of each dimension for employees' compliance with the organizational information security policy. Thus, the developed scale helps researchers and security managers alike to measure security-related stress among staff and deal with its consequences.

The paper continues as follows: First, we provide a review of previous IS stress research. Building on this, we subsequently develop a comprehensive conceptualization of the security-related stress construct with its different sub-dimensions. We then give insights into each step of the scale development procedure spanning item generation, the assessment of content validity, scale evaluation, and scale refinement. Finally, we discuss our study's contributions, implications, and limitations.

Related Work

In this section, we present prior IS stress research in its three succeeding stages: early research with focus on the job stress of IS personnel, research in the field of technostress, and finally research on security-related stress.

Early IS Stress Research

Early IS stress research (e.g. Ivancevich et al. 1985; Li and Shani 1991; Moore 2000; Weiss 1983) focuses on the occupational stress of IS professionals. Work overload, which can be defined as "too much work or work that is beyond one's capability" (Weiss 1983), is reported as common in the work environment of IS staff (Ivancevich et al. 1985). Li and Shani (1991) as well as Moore (2000) identify this work overload as the major stressor among IS personnel. Weiss (1983) identifies technological change as, among others, a germane stressor, which she refers to as "keeping up with rapid changes in the information processing field".

IS Technostress

Building on early IS stress research, during the last decade, as information and communication technology gradually spread into everyday life, substantial research was conducted in the field of technostress (e.g. Ayyagari et al. 2011; Galluch et al. 2015; Ragu-Nathan et al. 2008; Tarafdar et al. 2010). Technostress is a phenomenon that occurs when being confronted or working with new technologies. It can be described as an "inability to cope with the new technologies in a healthy manner" (Brod 1984). Measurement of technostress divides into survey-based measurement approaches (e.g. Ayyagari et al. 2011; Ragu-Nathan et al. 2008; Tarafdar et al. 2010) and neurobiological experiments (e.g. Galluch et al. 2015; Riedl 2013; Riedl et al. 2012). As we share the same measurement approach, we focus on the former.

Tarafdar et al. (2007) develop a model, which investigates the impact of technostress on individual productivity and role stress. Employing factor analysis, they identify five technostress creators, namely techno-complexity, techno-insecurity, techno-invasion, techno-overload, and techno-uncertainty. These technostress creators find further application in other studies such as Ragu-Nathan et al. (2008) or Tu et al. (2005). Table 1 contains definitions on these creators of technostress.

Stressor	Definition
Techno-complexity	Employees have to invest time and effort to understand and learn how to work with new technologies. Thereby, confusion results from jargon, a 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 about technologies.

Table 1. Creators of Technostress by Tarafdar et al. (2007)

Relying on the Person-Environment (P-E) fit model, Ayyagari et al. (2011) shed light on the individual importance of technology characteristics concerning technostress. They discuss the stressors work overload, role ambiguity, job insecurity, work-home conflict, and privacy invasion. All except privacy invasion are found to be relevant. For detailed definitions, see Table 2.

Stressor	Definition
Work overload	An individual's perception that assigned work exceeds own abilities and skills.
Role ambiguity	The unpredictability of the consequences of one's role performance, as well as the lack of information, needed to perform the role.
Job insecurity	The threat of job loss an individual perceives and faces.
Work-home conflict	An individual's perceived conflict between the demands of work and family.
Invasion of privacy	The perception that individual's privacy is compromised.

Table 2. Creators of Technostress by Ayyagari et al. (2011)

Security-Related Stress

Only recently, IS stress research extended into the field of behavioral information security. To the best of our knowledge, so far, there have been merely two studies on stress resulting from information security requirements (D'Arcy et al. 2014; Lee et al. 2016). Both studies transfer the construct of technostress to the context of information security.

First, D'Arcy et al. (2014) are longing to better understand employees' response to stressful information security requirements. Based on coping and moral disengagement theory, they explore security-related stress and its relationship to intentional violations of information security policies. Drawing on former technostress research, they investigate a three-dimensional view of security-related stress. They consider the aspects security-related complexity, security-related overload, and security-related uncertainty, which they describe as defined in Table 3. The findings confirm that stress from information security requirements increases moral disengagement and, consequently, security policy violations (D'Arcy et al. 2014).

Second, Lee et al. (2016) approach the topic of security-related stress based on the P-E fit theory and using a transaction-based perspective. They assume the stressors for security-related stress to be identical to those of job stress and technostress and employ work overload as well as privacy invasion, which they define in unison with Ayyagari et al. (2011, Table 2). The results confirm the relevance of the two stated information security stressors and further reveal that work overload has a greater effect in managerial security-oriented organizations. Moreover, the study shows that a compliant attitude towards information security policy mitigates work overload and privacy invasion.

Stressor	Definition
Security-related complexity	Employees have to invest extra time and effort to understand and apply measures of information security. This is enforced, for instance, by contingencies or jargon.
Security-related overload	Information security requirements increase the workload of the staff members. They have to accomplish more work in less time.
Security-related uncertainty	Employees are confronted with continuous changes with respect to information security requirements, thus are kept from developing an experiential information security basis as they have to regularly refresh their information security knowledge.

Table 3. Creators of Security-Related Stress by D'Arcy et al. (2014)

To sum up, past work has increasingly studied technostress and also first studies on security-related stress exist. However, the existing studies on security-related stress exclusively deduce from technostress research and concentrate on the stressors complexity, overload, and uncertainty (D'Arcy et al. 2014) as well as overload and privacy invasion (Lee et al. 2016), while they neglect further stressors emerging in the security context. As suggested in Ament and Haag (2016), we argue that the particular security-related environment generates additional stressors on employees that need to be considered when analyzing and measuring security-related stress. Therefore, in the next sections, we develop a comprehensive multidimensional construct of security-related stress that includes security-specific dimensions emerging in people's work, personal, and social environment.

Conceptualization

At the first stage of the scale development procedure, the concept of security-related stress needs to be developed (MacKenzie et al. 2011). In line with former IS stress research (e.g. Tarafdar et al. 2007), we expect security-related stress to be a multidimensional construct consisting of conceptually distinct, but interrelated sub-dimensions, i.e., we assume a reflective first-order, reflective second-order construct (Polites et al. 2012). Thus, each sub-dimension is reflected by its interchangeable indicators and captures a unique facet of the theoretical concept of security-related stress manifested in a specific relationship with the overarching second-order construct.

To identify all relevant sub-dimensions, we first build on prior IS stress research as outlined above, in particular, on the creators of the technostress constructs developed by Tarafdar et al. (2007) and Ayyagari et al. (2011) as well as those of security-related stress used by D'Arcy et al. (2014), see Table 1 through 3. Additionally, to verify these stressors and, in particular, to identify new stressors specific to the information security context, we conducted expert discussions and voluntary target group interviews in a large-scale enterprise of the financial industry. We posed a set of broad, open-ended questions to three professionals in the field of IS security. The questions were designed to collect wide, security-related knowledge of the experts. In a second round of discussions, we went into more detailed questions. Furthermore, we carried out more than 50 interviews (each lasting approximately 30 minutes) with representatives of the target group, i.e., employees confronted with information security requirements during their everyday work, about their security-related perceptions. The interviews were guide-based, thus of a semi-structured nature, allowing for new ideas and consequently original approaches. The cooperating company as well as the individual interviewees were assured of anonymity and confidentiality [1]. Conducting expert discussions and interviews allowed us to recognize necessary and substantial aspects of security-related stress not directly observable (MacKenzie et al. 2011).

As a result of the discussions, the interviews, and the literature review, we identified eight potential stressors of security-related stress, which we categorized into three different groups as displayed in Figure 1: stressors regarding employees' work, personal, and social environment. Thus, in addition to the existing five dimensions discussed so far in IS stress literature, we revealed three utterly new stressors (shaded in Figure 1) related to the themes of degree of freedom, conflict, and news. In the following, we describe each of the stressors in more detail.

[1] More details on the interviews and their results can be requested from the authors.

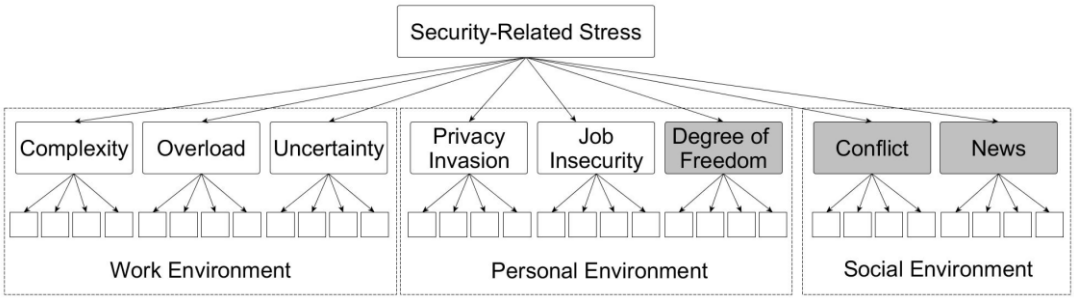

Figure 1. Proposed Reflective First-, Reflective Second-Order Construct of Security-Related Stress

Security-Related Stress Regarding Employees' Work Environment

Staff members may encounter security-related stress resulting from their work environment with regard to complexity, overload, and uncertainty. These three stressors are established in prior research (Tarafdar et al. 2007) and are the equivalent to the security-related stress construct of D'Arcy et al. (2014).

Security-Related Stress from Complexity

Information security increases employees' job demands by enforcing additional constantly changing requirements (Albrechtsen and Hovden 2009). Consequently, employees have to spend time and effort on learning, understanding, and implementing those information security requirements. Furthermore, the complexity of security requirements possibly exceeds an employee's intellectual abilities. For example, personnel might be unable to cope with information security in terms of secure data communication. Encrypting and decrypting emails or establishing a safe data connection to a company's intranet might be challenging and thus, as an employee depends on such security knowhow to appropriately fulfill his work, impose security-related stress.

In the words of the P-E fit model, the demands of the environment might be greater than an employee's abilities (Ayyagari et al. 2011). This can lead to problems of understanding or even to misunderstandings (D'Arcy et al. 2014). Interview partners pointed out that they fear to unintentionally cause an information security breach. Besides, they are afraid of taking responsibility for information security decisions. Therefore, we expect complexity to represent one dimension of security-related stress.

Security-Related Stress from Overload

Identified as the most important IS stressor in the past (e.g. Li and Shani 1991; Moore 2000), work overload should also be of relevance in the context of security-related stress (D'Arcy et al. 2014; Lee et al. 2016). For example, our target group interviewees most frequently cited password management as one important security-related stressor. Often employees have to handle a tremendous amount of passwords, which all have to differ and comply with a company's security policy. Another example of security-overload is the need to constantly de- or encrypt emails before reading or sending respectively.

Due to information security requirements, employees have to fulfill additional tasks and are confronted with more work than they can handle. A conflict of interest between functionality and security emerges as the workload regarding information security increases (Albrechtsen 2007). The application of security controls puts pressure on the employees, which may need to maintain the same performance level than prior to the introduction of information security requirements (Posey et al. 2011). As a consequence, they are forced to work faster to fulfill their actual tasks in time, which might lead to a decrease in working quality. Alternatively, employees have to suffer longer working hours. In addition, information security measures could interrupt the routine workflow and lead to multitasking.

Security-Related Stress from Uncertainty

As a consequence of rapid technology developments, which is proven to be a stressor to IS personnel (Weiss 1983), technical and behavioral information security is in constant transition. This includes changes of information security policies and procedures, information security requirements, and information security technologies alike (D'Arcy et al. 2014). Employees have to continuously update their security knowledge, which prevents them from building a solid security routine, as stated by several interview partners. This describes security-related stress created from uncertainty.

Security-Related Stress Regarding Employees' Personal Environment

Besides complexity, overload, and uncertainty, which focus on employees' work environment, stressors concerning the personal environment are important when developing a complete construct of security-related stress. We identified privacy invasion, job insecurity, as well as the degree of decision freedom due to information security as creators of stress in terms of personal environment.

Security-Related Stress from Invasion

Invasion of privacy is, similar to the above-mentioned factors, a creator of technostress (Ragu-Nathan et al. 2008; Tarafdar et al. 2007). However, previous research in the field of security-related stress is at odds with its definition and consequently its relevance. While Lee et al. (2016) interpret privacy invasion in terms of information security as monitoring an employee's behavior – if required technology is at hand – D'Arcy et al. (2014), who deduce from the technostress construct of Tarafdar et al. (2007), reject the stressor's importance due to great conceptual overlapping with the three stressors which we discussed above.

During our expert discussions and target group interviews we found that invasion in the context of information security does not fit with the definition of Tarafdar et al. (2007) in the context of technostress referring to spending leisure time on information security. A more appropriate definition in the security context seems to be one in line with Ayyagari et al.'s (2011) definition of technostress invasion of privacy. Accordingly, in the context of security-related stress, the stressor invasion may focus on behavioral monitoring and the tracking of information security behavior. This can, for instance, include monitoring staff members' Internet usage or email traffic. Employees are stressed because they fear that their employer could violate their privacy. Aiello and Kolb (1995) as well as Smith et al. (1992) present details on occupational stress due to electronic performance monitoring. We label this dimension as security-invasion.

Security-Related Stress from Job Insecurity

Moreover, information security measures can result in job insecurity. Employees work assessment might include an evaluation of their information security behavior and ISP compliance in addition to the quality and quantity of their task fulfillment. The concern to fulfill assignments disaccording to expectations leads to stress. Young (2010), for instance, argues that an employee who caused a severe security incident might face job loss. Interview partners stated that as job demands increase, employees compete in terms of job qualifications. Staff members might feel threatened by co-workers with better information security skills. This can result in less sharing of knowledge among co-workers as they fear replacement. Although interviewees did not completely agree on this topic, experts see this form of security-stress to further emerge within the next years as job qualifications proceed to alter. Therefore, we suggest job insecurity as a conceivable creator of security-related stress.

Security-Related Stress from Degree of Freedom

Employees frequently face security-critical situations which they have not been prepared for, as they are not covered by information security policy or training. Because wrong information security decisions can have severe consequences, interviewees stated that they commonly turn to internal help desks, security officers, or their principals. Sometimes employees might also be left in charge of security decisions themselves. Such responsibility leads to occupational stress. This is, in particular, true for personnel with a relatively low self-efficacy since they more strongly question their own capabilities (Matsui and Onglatco 1992).

On the contrary, employees might have to change their way of working when including security procedures in their working routine. Hence, they could feel constrained in their freedom of decision and their innovativeness due to information security requirements, which in turn induces stress. Altogether, security-related stress can arise from the freedom to decide, but also from restrictions. Employees either have to handle responsibility, which might be accompanied by certain consequences, or are limited in their autonomy.

Security-Related Stress Regarding Employees' Social Environment

Finally, interviewees and experts mentioned two additional stressors in the field of information security, which we classified as stress due to employees' social environment because employees might feel stressed when interacting with others. Accordingly, security-related stress can be triggered by conflicts or news.

Security-Related Stress from Conflict

Conflicts are a common, but in IS stress research disregarded, workplace stressors (Ongori and Agolla 2008). Conflicts can arise when instructions of supervisors or requests by peers are not in line with established information security requirements. Employees feel stressed because they have to either violate existing regulations or face confrontation with colleagues. For example, if security policies prohibit sharing computer passwords, an employee, who will be on leave, could refuse to give his login credentials to the colleague who is supposed to be his vacation replacement. This might lead to an argumentation on common practice which can in turn stress the affected employee.

Security-Related Stress from News

A final stressor, which research has not yet considered, is stress from security-related news. Interview partners state that they feel unsettled when hearing about substantial security breaches or the misuse of sensitive data. The magnitude thereby varies depending on the information source, i.e., if the information is presented by close friends, colleagues, or mass media. Additionally, the individual relevance, which most often comes down to whether oneself is directly affected, influences the stress level. An employee who makes use of the same hard- or software, identified to have a security gap, is more likely to experience security-related stress.

Further substantiation of this stressor's relevance gives the theory of fear appeals (e.g. Rogers 1975). The theory of fear appeals describes how a persuasive message containing the element of fear affects the behavioral intention of users (Johnston and Warkentin 2010). Therefore, we propose security-related stress as the eighth and final dimension of the multidimensional security-related stress construct.

Development of Measures

Based on this conceptualization, we next developed a set of items in order to operationalize the multiple dimensions of the security-related stress construct. As far as applicable, we adopted items from related work and adapted them to the context of security-related stress. For the remainder, we generated new items inductively. We end this section by evaluating items' content validity.

Item Generation

During the item generation process, we developed items for each individual sub-dimension and meanwhile kept an eye on these items being essential for the focal construct's definition (MacKenzie et al. 2011). In line with D'Arcy et al. (2014) and Lee et al. (2016), we included items respectively from Ragu-Nathan et al. (2008) and Ayygari et al. (2011) and adjusted them to the context of security-related stress.

To fully and properly operationalize the theoretical concept of security-related stress, we also generated new indicators reflecting the identified dimensions that have been left out of consideration in prior research that are degree of freedom, conflict, and news. In doing so, we referred to each dimension's conception as presented in the previous section above and carefully took into account that items are kept simple, precise, and unambiguous (Hinkin 1998). We terminated this stage of research methodology with a broad initial set of items.

#	Item
Overload	
1	I am forced by information security policies and procedures to do more work than I can handle.
2	Due to information security requirements, I do not have enough time to fulfill my actual tasks.
3	Means of information security force me to work faster.
4	Information security workload sometimes hinders me to perform my actual tasks in time.
5	I have a higher workload due to information security requirements.[2]
News	
6	Reports on information security gaps unsettle me.
7	I feel at risk when hearing about information security gaps.
8	I feel at risk when hearing about information security incidents.
9	Reports on information security incidents unsettle me.
Uncertainty	
10	There are constant changes in security-related technologies in my organization.
11	There are constant changes in information security policies and procedures in my organization.
12	There are always new and unpredictable information security requirements in my job.
13	If information security requirements constantly change I cannot build up a solid security routine.[2]
Privacy invasion	
14	Controlling my information security behavior is an invasion of my privacy.
15	I feel uncomfortable that my information security behavior can be easily monitored.
16	I feel my employer could violate my privacy by tracking my information security behavior.
Complexity	
17	I am likely to unintentionally cause an information security breach.
18	It takes me a while to understand and regard my organization's information security policies and procedures.
19	I often find it difficult to understand and regard my organization's information security policy.
Conflict	
20	Working instructions which are not in line with the organization's information security policy pressure me.
21	It pressures me if colleagues ask me to break the organization's information security rules.
22	I often find information security rules contrary to my actually assigned tasks.[2]
23	In my organization colleagues think poorly of those who tightly follow the information security policy.[2]
Job insecurity	
24	I would face job loss if I caused a consequential breach of information security.[2]
25	I feel threatened by co-workers with better information security skills.[2]
26	I have to constantly update my information security skills to avoid replacement.[2]
27	My performance review includes my information security adherence.[2]
Degree of freedom	
28	I fear taking responsibility for information security decisions.[3]
29	My innovative thinking at work declines due to information security requirements.[2]
30	I feel restricted in my freedom of decision at work due to my organization's information security requirements.[2]

Table 4. Items of Security-Related Stress

[2] These items were deleted during the subsequent EFA.
[3] This item was deleted during the subsequent CFA.

Assessment of Items Content Validity

After the item generation phase, we checked the items' content validity, which is "the degree to which items in an instrument reflect the content universe to which the instrument will be generalized" (Straub et al. 2004). For this purpose, we used the technique employed by MacKenzie et al. (1991). We asked five persons distinct in their substantial understanding of information security to classify the randomly ordered items. In addition, we provided them with an "other" dimension as well as a comment field. Items were retained only if 80% of participants (four out of five) assigned them correctly (MacKenzie et al. 1991). Furthermore, we asked five persons from the target audience to comment on the relevance of the questions for the context of security-related stress as well as to assess the questions' unambiguousness. We adjusted the items and sorted out those that failed to meet the mentioned criteria. We established a set of 30 items for further evaluation and refinement (see Table 4).

Scale Evaluation and Refinement

After identifying the model by fixing one regression weight to 1.0 in each measurement scale (MacKenzie et al. 2011), we carried out a pretest to evaluate the instrument and examine the scales' convergent, discriminant, and nomological validity. With the collected data, we conducted an exploratory factor analysis (EFA), a confirmatory factor analysis (CFA), and finally employed structural equation modeling (SEM) to assess the relation of the developed security-related stress construct with employees' intention to comply with information security measures, an important construct of its theoretical network (e.g. Bulgurcu et al. 2010; Siponen and Vance 2010).

Pretest Data Collection

To pretest the scale, we set up a questionnaire. The questionnaire included the generated security-related stress items (Table 4), established measures of employees' compliance with the information security policy (Bulgurcu et al. 2010), and demographic information. We also integrated questions in the form of reversed items to control for respondents' attention. Descriptions of potentially unfamiliar terms were provided to improve the response quality. All items were measured on a five-point Likert scale from 1 ("strongly agree") to 5 ("strongly disagree").

		Frequency	Percentage
Gender	Female	66	40%
	Male	99	60%
	Total	165	100%
Work experience (in years)	< 6	116	70%
	6 – 15	30	18%
	> 15	19	12%
	Total	165	100%
Education	Bachelor's degree	62	38%
	Master's degree	69	42%
	Others	34	21%
	Total	165	100%
Company size (# of employees)	< 50	23	14%
	50 – 249	31	19%
	250 – 999	16	10%
	1.000 – 4.999	27	16%
	> 5.000	68	41%
	Total	165	100%

Table 5. Sample Characteristics

Emails, which asked for participation, described the nature as well as the purpose of the study, and provided the link to the online version of the survey, were sent out to 277 potential participants from the researchers'

social networks. Altogether, 175 online surveys were submitted (response rate of 63.2%). In addition, a class of 40 master students with work experience was asked to fill out a paper-based version of the questionnaire. All participants, regardless of whether they filled out the online or paper-based questionnaire, were informed that the survey was voluntary and they were assured that responses would be treated confidentially and anonymously.

We filtered out participants who did not fit the target group (i.e., employees confronted with information security requirements on a frequent basis). Besides, we excluded incomplete data sets. Out of the collected 215 data sets, 165 were used as the final sample for the pretest. This sample size is deemed to be sufficient for a pretest and scale validation (MacKenzie et al. 2011; Hinkin 1998).

Selected sample characteristics are presented in Table 5. 60% of the participants are males. Furthermore, the relatively high education standard of the participants is mentionable. At the same time, respondents have a rather low work experience, and a majority works in companies with more than 5,000 employees.

Scale Purification and Refinement

With this collected data, we subsequently refined and validated the construct. Using IBM SPSS Statistics 21 and SPSS Amos 21, we conducted an exploratory factor analysis (EFA) as well as a confirmatory factor analysis (CFA), and finally structural equation modeling (SEM) to assess the construct's nomological validity.

#	Rotated component matrix						Reliability	Mean	Standard deviation
Overload							0.871	4.079	0.873
1	0.865								
2	0.806								
3	0.696								
4	0.754								
News							0.880	2.789	1.066
6		0.873							
7		0.843							
8		0.798							
9		0.796							
Uncertainty							0.825	3.311	1.105
10			0.861						
11			0.854						
12			0.733						
Privacy invasion							0.728	3.560	1.097
14				0.806					
15				0.765					
16				0.714					
Complexity							0.730	3.391	1.102
17					0.701				
18					0.699				
19					0.646				
28					0.603				
Conflict							0.722	2.821	1.225
20						0.793			
21						0.765			

Table 6. EFA Results

Exploratory Factor Analysis

We conducted an exploratory factor analysis using IBM SPSS Statistics. An EFA allows reducing the number of observed variables to fewer unobserved factors. Consequently, the interpretability is improved and hidden data structures are revealed (Treiblmaier and Filzmoser 2010).

The results of the EFA suggested dropping all items related to the stressor insecurity. These items did not load together as a sub-construct and thus seem to be less important for the security-related stress construct. This is in line with our mixed findings during the initial interview phase. Furthermore, we eliminated most of the items generated to capture stress due to degree of freedom as they could not be clearly assigned to one of the sub-dimensions. Another four items, which did not properly load on any factor or were subject to cross-loadings, had to be dropped during the analysis (footnote 2 in Table 4). Out of the remaining 20 items, the EFA retained a six-factor structure. Each of these six factors was considered as a unique sub-dimension of security-related stress.

Table 6 includes details on the six factors' rotated component matrix, factor reliability (Cronbach's alpha), mean, and standard deviation. Factor loadings of the items were well above the recommended minimum value of 0.5. No substantial cross-loadings existed. All factors showed a Cronbach's alpha above the threshold of 0.7 (Straub et al. 2004). We checked for convergent validity and revealed that items of one sub-dimension are sufficiently correlated. Moreover, we established discriminant validity because the indicators are distinct and uncorrelated towards other factors than their own (MacKenzie et al. 2011).

Confirmatory Factor Analysis

As a next step, we performed a confirmatory factor analysis to approve the factor structure identified during the EFA. The six sub-factors were modeled into a second-order construct of security-related stress. We conducted the CFA using IBM SPSS Amos. In the course of this, item 28 (footnote 3 in Table 4) had to be dropped due to validity issues.

	χ^2	df	χ^2/df	GFI	AGFI	NFI	CFI	RMR
Model 1	163.711	140.000	1.169	0.906	0.873	0.892	0.982	0.083
Model 2	154.307	137.000	1.126	0.912	0.879	0.899	0.987	0.062
Model 3	156.173	139.000	1.124	0.911	0.878	0.897	0.987	0.070

Table 7. Model Fit Indices of the CFA

To verify the six-factor structure of the second-order construct of security-related stress (Model 1, see Figure 1), we compared it with several first-order constructs (Model 2) representing a correlated model which treats each of the six sub-dimensions of security-related stress as a single latent construct. Furthermore, we tested a model of security-related stress, which is composed of three separate latent constructs (Model 3), representing first, a second-order construct of security-related stress from employees' work environment, including the three sub-dimensions complexity, overload, and uncertainty, second, a first-order latent construct representing security-related stress, resulting from employees' personal environment manifested in privacy invasion, and third, a second-order construct of security-related stress, resulting from employees' social environment, including the two sub-dimensions news and conflict (see Figure 2). The inter-construct relationships in all three models showed statistical significance and the model fit indices of all three models exceeded the recommended threshold values (compare Hadjistavropoulos et al. 1999; Hair et al. 2010; Hu and Bentler 1999), see Table 7. To verify the multidimensional structure, the ratio of the χ^2 of a first-order model to the χ^2 of a higher order model should exceed 80% (Marsh and Hocevar 1985). This applies for both, Model 1 and Model 3, with Model 1 having a target coefficient of 94.26% and Model 3 a target coefficient of 98.81%. Besides, measures of composite reliability, convergent validity, and discriminant validity are within the suggested ranges (Hair et al. 2010) for Model 1 as well as for Model 3. Thus, the CFA proved evidence of the second-order construct and as Model 3 performs better than Model 1 with respect to all key figures, we used this proposed and adjusted model of security-related stress (i.e., Model 3 as displayed in Figure 2) for structural equation modeling.

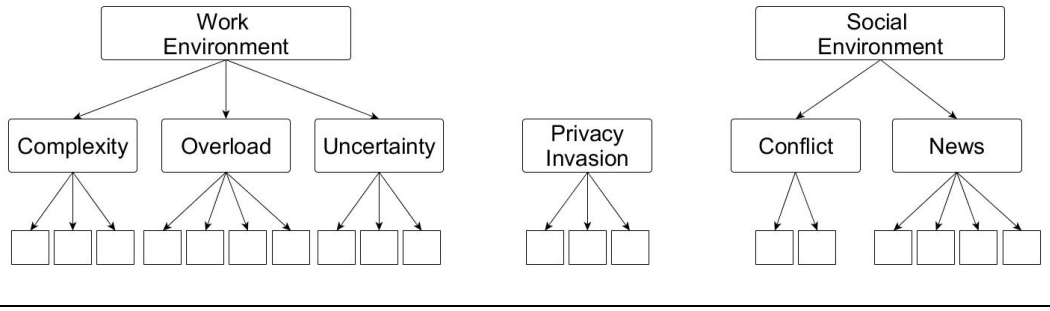

Figure 2. Final Measurement Model of Security-Related Stress (Model 3)

Structural Equation Modeling

Finally, we embedded the construct into its nomological network (MacKenzie et al. 2011) to assess the relationship of the developed security-related stress construct with one of the most important constructs of its theoretical network and thus evaluate the construct's nomological validity. As prior behavioral IS security research links security-related stress with employees' ISP compliance (D'Arcy et al. 2014), our security-related stress construct (see Figure 2) is proposed to influence ISP compliance intention. While further correlations, for instance, with the closely related construct of technostress (Ament and Haag 2016), individuals' productivity or performance (Ament and Haag 2016; Hung et al. 2011; Tarafdar et al. 2007; 2010), job satisfaction (Ragu-Nathan et al. 2008; Tarafdar et al. 2010), or security awareness (Bulgurcu et al. 2010) are conceivable, in this paper, we exemplarily concentrate on employees' ISP compliance intention, which is found to be a close representative of individuals' actual behavior in general (Fishbein and Ajzen 1975) and of individuals' actual compliance with information security policy in particular (e.g. Bulgurcu et al. 2010; Siponen and Vance 2010). ISP compliance intention is defined as the intention to comply with information security requirements in the future, i.e., to protect the IS resources and to respect the own security responsibility as described in the given information security policy (Bulgurcu et al. 2010).

Bulgurcu et al. (2010) state that work impediments, such as stress, increase the perceived cost of complying, which in turn leads to a lower ISP compliance intention. D'Arcy et al. (2014) find, as stated above, a positive indirect relationship between security-related stress and violation intention through moral disengagement. Thus, we hypothesize that security-related stress has a negative effect on employees' ISP compliance intention. Or put differently, our security-related stress construct (see Figure 2) is proposed to decrease employees' ISP compliance intention.

χ^2	df	χ^2/df	GFI	AGFI	NFI	CFI	RMR
286.476	198.000	1.447	0.862	0.824	0.840	0.943	0.122

Table 8. Model Fit Indices of the SEM

To test this relationship, we built a structural model by including the construct of ISP compliance intention. Table 8 provides the results of the SEM. Comparing the model fit indices against the recommended thresholds (Hadjistavropoulos et al. 1999; Hair et al. 2010; Hu and Bentler 1999) proved the fit of the model. In addition, all resulting path coefficients were significant (Figure 3). As we verify a newly constructed measure, a loading of approximately 0.5 between work environment and the evidentially important sub-construct uncertainty (D'Arcy et al. 2014) is acceptable (MacKenzie et al. 2011). Thus, the SEM supports our expectation that security-related stress is significantly related to ISP compliance intention. However, while stressors of the work environment as well as privacy invasion, which is stress from the personal environment, decrease ISP compliance intention in the expected way, the effect of stressors of the social environment, namely conflict and news, is reversed and significantly strengthens ISP compliance intention.

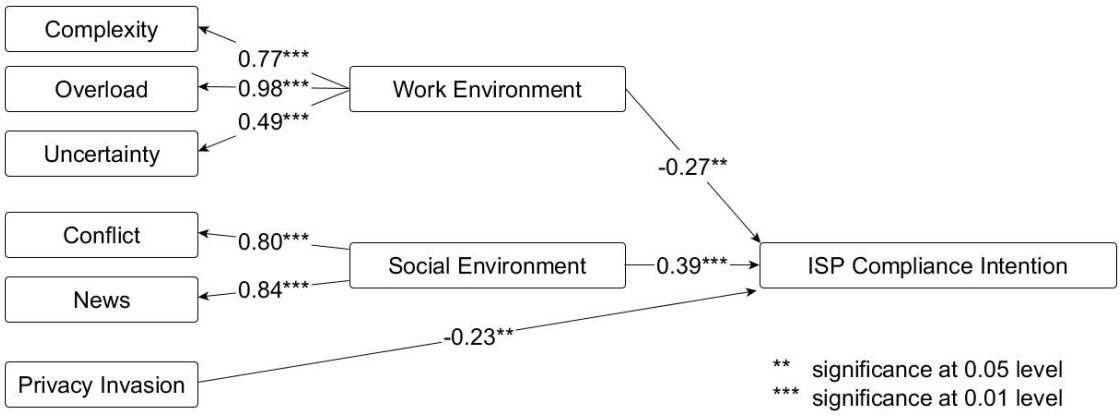

Figure 3. SEM Results

Discussion

In this paper, we combine insights from information security and IS stress research to develop and validate a comprehensive construct of security-related stress spanning employees' work, personal, and social environment. Our work provides important contributions to and implications for theory as we show detailed conceptual and empirical findings on the side-effect of information security measures. In addition, the research results provide practitioners with a toolset in terms of security-related stress. In the following, we will discuss those contributions and implications together with the paper's limitations and promising future research directions.

Contributions and Implications

Our key contribution is the comprehensive conceptualization of security-related stress, which combines and extends the existing knowledge base from two distinct research fields, namely information security and IS stress research. Whereas previous approaches have directly transferred the technostress dimensions to the context of information security, we present a more comprehensive construct of security-related stress adding and emphasizing the specific aspects of an information security setting. The final construct comprises six stressors, including the newly identified stressors conflict and news, from three different categories, namely employees' work, personal, and social environment. Although prior work has discussed security-related stress due to complexity, overload, uncertainty, and privacy invasion (D'Arcy et al. 2014; Lee et al. 2016), we are the first to merge and empirically validate all sub-dimensions into one comprehensive model.

Furthermore, we developed and tested a measurement instrument of this multidimensional security-related stress concept. The instrument consists of items of related work, which we adjusted to the security context, but also newly introduced items, which we generated inductively. The latter ones were developed based on more than 50 interviews with employees as well as expert discussions. We assessed the items' content validity with q-sorting. To validate our scale of security-related stress, we conducted a pilot study with data from 165 participants.

The refinement and validation processes during the EFA could not confirm the sub-constructs insecurity and degree of freedom as suggested by previous research (Young 2010) and our interviews with experts and employees. So, at least in our study, employees do not perceive security-related stress in terms of job insecurity. One explanation might be that although respondents state that they might lose their job if they cause a consequential information security breach, performance evaluation as well as the competition for qualification, do not – yet – include the factor information security. Security-related stress from job insecurity might gain more relevance over the next years as job qualifications proceed to alter in a way that not only broad knowledge on the usage of information and communication technology but also related

security provisions become obligatory. Similar is true for the degree of freedom. We found no empirical validation that employees feel security-related stress from limitation or autonomy. We encourage future research to re-test this lack of importance of job insecurity and decision freedom for employees' security-related stress.

During the CFA, the measure's structure was adjusted towards three separate latent constructs represented by two second-order constructs and one first-order construct (see Figure 2). With the help of SEM, we started embedding the developed construct into its nomological network. The first results of the SEM revealed interesting insights into the relationship between security-related stress and information security policy compliance intention. While we can confirm that work environment-related stress from complexity, overload, and uncertainty has a significant negative effect on employees' ISP compliance intention (D'Arcy et al. 2014) and add an equal substantial effect of privacy invasion, the social environment security-related stress construct, consisting of the sub-dimensions conflict and news, has a significant positive effect on ISP compliance intention. To be more specific, employees, which feel stressed if instructions of supervisors or requests by peers are not in line with established information security requirements, tend to behave more in line with information security requirements. The same is true for employees that feel stressed when hearing news or reports on information security incidents. Consequently, our study reveals that security-related stress does not only have a negative effect, but also a positive, and thus, an overall mixed effect on ISP compliance intention. Therefore, corresponding with technostress research which also found positive as well as negative outcomes of employees' perceived stress (Tu et al. 2005), our study reveals that experiencing some specific aspects of security-related stress can also be positive for the security of information systems. This coincides with the theory of fear appeals. Negative messages which contain an element of threat can lead to a higher ISP compliance among staff (Johnston and Warkentin 2010). Future research might build on this result and re-assess the opposite effects in an inductive way.

Besides implications for research, we provide practical implications important for decision-makers. This work supplies managers with the necessary toolset to recognize security-related stress among their staff. Due to the comprehensive set of stressors and the developed scale, security managers can more precisely identify the actual source of security-related stress, anticipate its effects while developing security policies, and, thus, adopt countermeasures or even avert security-related stress before it emerges. Regarding our findings with respect to the social environment, security-related stress might also be used as a security measure itself to sensitize employees.

To counteract security-related stress, our findings suggest an information security strategy, which focuses on the individual employee. Adequately formulated security policies, thus unambiguous and easy to understand, can reduce security-related stress from complexity. Furthermore, information security training and education should cover the content of information security policies and involved measures. Employees need a colleague as expert to consult if questions on the topic of information security arise. Besides, employees have to be informed about the relevance of information security and information security needs to be anchored in job descriptions. This way stress in terms of overload declines. In an organization with a positive and constructive working atmosphere employees, which are well educated with respect to information security, will be confident enough to confront their principal or peer if information security is at risk. Those responsible can transform security-related stress into a useful security source if they keep in mind that security related stress has favorable aspects. A proper reaction to current information security discussions or news, for instance, via newsfeeds, is necessary. Stress from invasion can be encountered by increasing awareness among employees and educating them to understand the importance of information security. If employees act in line with information security requirements, there is no need for monitoring their security behavior and thus no stress from privacy invasion.

Limitations and Future Research

As with any study, our findings need to be evaluated in terms of their limitations, which provide opportunities for future research.

Most importantly, the presented study is a first test of the security-related stress construct. This paper puts its attention on the development and first validation of a comprehensive security-related stress construct and its relation to ISP compliance intention. Thus, further validation with data from a new sample as well as reexamining the scale properties is essential (MacKenzie et al. 2011). Future studies on security-related stress can make use of our results, first, by validating our identified mixed impact of security-related stress,

and second, by employing the developed measure of security-related stress for their research endeavors. A longitudinal study seems promising to examine whether the mixed effect of security-related stress on ISP compliance intention is stable over time.

In addition, the relationship of the stress construct with other concepts of its nomological net should be assessed. Related work proves the effect stress constructs have on different target variables other than ISP compliance intention, such as individual productivity or performance (Ament and Haag 2016; Hung et al. 2011; Tarafdar et al. 2007; 2010) and job satisfaction (Ragu-Nathan et al. 2008; Tarafdar et al. 2010). Moreover, the construct's relationship with other independent variables, such as user involvement, found to be important in prior research (Ragu-Nathan et al. 2008; Tarafdar et al. 2010), should be valuable (MacKenzie et al. 2011). Furthermore, analyzing individual characteristics in this regard is of interest (Srivastava et al. 2015). A final promising aspect to examine in this context is the link with technostress (Ament and Haag 2016).

Moreover, the results of our study are limited by the selection of participants. During measurement development, we worked with interviewees from a single company and, for the purpose of scale evaluation and refinement, we focused on a broad sample from our social network. To control for the utilized information security strategy in a more detailed way, research in future might work with a sample of subjects from just one organization. A final issue is the self-reported, thus perceptual, nature of the collected data. Although it helped to ensure external validity, more objective research methods, relying on an experimental design, can be valuable in terms of stress measurement. Related work on technostress (e.g. Galluch et al. 2015; Riedl 2013; Riedl et al. 2012) may provide a good starting point for such research endeavors.

Conclusion

Recent research suggests that measures of information security have a negative effect on employees as they can cause stress (D'Arcy et al. 2014; Lee et al. 2016). Furthermore, first evidence shows that security-related stress drives information security policy non-compliance intention (D'Arcy et al. 2014). Building on and extending previous research, this work develops and empirically validates a comprehensive construct of individual-level security-related stress, including stress resulting from employees' work, personal, and social environment. In contrast to existent research providing only a negative view on security-related stress, this study presents researchers and practitioners with a multi-faceted perspective on security-related stress including both negative but also positive effects on ISP compliance intention.

References

Aiello, J. R., and Kolb, K. J. 1995. "Electronic Performance Monitoring and Social Context: Impact on Productivity and Stress," *Journal of Applied Psychology* (80:3), pp. 339–353.

Albrechtsen, E. 2007. "A Qualitative Study of Users' View on Information Security," *Computers & Security* (26:4), pp. 276–289.

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

Ament, C., and Haag, S. 2016. "Security-Related Stress: A Neglected Construct in Information Systems Stress Literature," *in Proceedings of the 24th European Conference on Information Systems (ECIS 2016)*, Istanbul, Turkey.

Ayyagari, R., Grover, V., and Purvis, R. 2011. "Technostress: Technological Antecedents and Implications," *MIS Quarterly* (35:4), pp. 831–858.

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

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.

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.

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Reading, MA, USA: Addison-Wesley.
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* (16:1), pp. 1–47.
Guo, K. H. 2013. "Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis," *Computers & Security* (32), pp. 242–251.
Hadjistavropoulos, H. D., Frombach, I. K., and Asmundson, G. J. (1999). "Exploratory and confirmatory factor analytic investigations of the Illness Attitudes Scale in a nonclinical sample," B*ehaviour Research and Therapy* (37:7), pp. 671-684.
Hair, J., Black, W., Babin, B., and Anderson, R. 2010. *Multivariate Data Analysis*, Upper Saddle River, NJ, USA: Prentice Hall.
Hinkin, T. R. 1998. "A Brief Tutorial on the Development of Measures for Use in Survey Questionnaires," *Organizational Research Methods* (1:1), pp. 104–121.
Hu, L. and Bentler, P.M. (1999). "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives," *Structural Equation Modeling* (6:1), pp. 1-55.
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, Australia, paper 81.
Ivancevich, J. M., Albert Napier, H., and Wetherbe, J. C. 1985. "An Empirical Study of Occupational Stress, Attitudes and Health among Information Systems Personnel," *Information & Management* (9:2), pp. 77–85.
Johnston, A.C. and Warkentin, M. (2010), "Fear Appeals and Information Security Behaviors: An Empirical Study", *MIS Quarterly*, (34:3), pp. 549–566.
Lee, C., Lee, C. C., and Kim, S. 2016. "Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity," *Computers & Security* (59), pp. 60–70.
Li, E. Y., and Shani, A. B. 1991. "Stress Dynamics of Information Systems Managers: A Contingency Model," *Journal of Management Information Systems* (7:4), pp. 107–130.
MacKenzie, S. B., Podsakoff, P. M., and Fetter, R. 1991. "Organizational Citizenship Behavior and Objective Productivity as Determinants of Managerial Evaluations of Salespersons' Performance," *Organizational Behavior and Human Decision Processes* (50:1), pp. 123–150.
MacKenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011. "Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques," *MIS Quarterly* (35:2), pp. 293–334.
Marsh, H. W., and Hocevar, D. 1985. "Application of Confirmatory Factor Analysis to the Study of Self-Concept: First-and Higher Order Factor Models and Their Invariance Across Groups," *Psychological Bulletin* (97:3), p. 562.
Matsui, T., and Onglatco, M.-L. 1992. "Career Self-Efficacy as a Moderator of the Relation between Occupational Stress on Strain," *Journal of Vocational Behavior* (41), pp. 79–88.
Moore, J. E. 2000. "One Road to Turnover: An Examination of Work Exhaustion in Technology Professionals," *MIS Quarterly* (24:1), pp. 141–168.
Ongori, H., and Agolla, J. E. 2008. "Occupational Stress in Organizations and Its Effects on Organizational Performance," *Journal of Management Research* (8:3), pp. 123–134.
Polites, G. L., Roberts, N., and Thatcher, J. 2012. "Conceptualizing models using multidimensional constructs: a review and guidelines for their use," *European Journal of Information Systems* (21:1), pp. 22–48.
Ponemon Institute. 2015. "*2015 Cost of Data Breach Study: Global Analysis*", (available at https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF; accessed on April 30, 2016).
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* (7:1), pp. 24–47.
Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757–778.
PWC. 2015. "*Turnaround and Transformation: Key Findings from the Global State of Information Security Survey 2016*", (available at http://pwc.com/gsiss; accessed on October 10, 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* (19:4), pp. 417–433.
Riedl, R. 2013. "On the Biology of Technostress: Literature Review and Research Agenda," *ACM SIGMIS Database* (44:1), pp. 18–55.
Riedl, R., Kindermann, H., Auinger, A. and Javor, A. 2012. "Technostress from a Neurobiological Perspective," *Business & Information Systems Engineering* (4:2), pp. 61–69.
Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91), pp. 93-114.
Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487–502.
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* (23:1), 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* (25:4), pp. 355–401.
Straub, D., Boudreau, M.-C., and Gefen, D. 2004. "Validation Guidelines for IS Positivist Research," *The Communications of the Association for Information Systems* (13:1), pp. 380–427.
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* (24:1), 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* (27:3), pp. 303–334.
Treiblmaier, H., and Filzmoser, P. 2010. "Exploratory Factor Analysis Revisited: How Robust Methods Support the Detection of Hidden Multivariate Data Structures in IS Research," *Information & Management* (47:4), pp. 197–207.
Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. 2013. "Managing the Introduction of Information Security Awareness Programmes in Organisations," *European Journal of Information Systems* (24:1), pp. 38–58.
Tu, Q., Wang, K., and Shu, Q. 2005. "Computer-Related Technostress in China," *Communications of the ACM* (48:4), pp. 77–81.
Weiss, M. 1983. "Effects of Work Stress and Social Support on Information Systems Managers," *MIS Quarterly* (7:1), pp. 29–43.
Young, K. 2010. "Policies and Procedures to Manage Employee Internet Abuse," *Computers in Human Behavior* (26:6), pp. 1467–1471.