Turun yliopisto
University of Turku

IMPROVING INFORMATION SECURITY PRACTICES TO REDUCE SECURITY-RELATED STRESS IN END-USERS

Master's Thesis in Information Systems Science

Author
Mari Mäkinen

Supervisor:
Ph.D. Jonna Järveläinen

18.12.2017
Turku

Table of contents

List of figures

List of tables

1 INTRODUCTION

1.1 Research area

The concept of technostress – meaning stress caused by information and communication technologies – initially emerged in the 1980s, around the same time as the first personal computers were introduced into organizational use (siop.org). The first scientific article on the topic dates back to 1982 (Brod 1982) and describes stress symptoms caused by situations such as an employee having to start using a word processing system or having a computer terminal placed near the employee's workstation. Nowadays technology plays a central role in organizations, and employees are constantly expected to develop and master new skills in new areas of technological innovation. It is nearly impossible to find a job posting that does not state some sort of technical skillset as a prerequisite for the applicant.

As information security incidents are on the rise (PWC 2015), the concept of technostress has been getting new dimensions. The exponential development rate of new technologies has brought along with it various and significant information security threats which organizations aim to fight against through information security policies and practices. Employees are expected to keep their information security knowledge and skills up to date with all the fast developments in both technology and cybercrime. Adopting new cybersecurity measures is causing stress in employees, and the results are detrimental to productivity (udel.edu 2014). Examples of stressful situations include having to remember a variety of passwords without storing them anywhere, being afraid of accidentally divulging confidential data or unintentionally causing a security breach (Ament & Haag 2016).

It is a common belief that employees are the biggest threat to information security in organizations (fortune.com 2016; forbes.com 2011). The little research that has been done on the topic of information security stress (D'Arcy et al. 2014; Ament & Haag 2016; Lee et al. 2016) has proven that the phenomenon exists in organizations and that the implications are serious. It is therefore evident that more research on what employees find stressful is needed. The topic it is a fairly new research area for information systems (IS) research, all the while presenting a very real threat to companies. The results and practical implications that can be drawn from this research are useful for companies – and especially their information security experts – because they can improve compliance and consequently the state of cybersecurity within the organization.

1.2 Research gap

There is large body of IS research on the topic of technostress. However the concept of security-related stress (SRS) (also dubbed information security stress (ISS), but the term security-related stress will be used for the purposes of this thesis as it's abbreviation is more distinct from other information systems abbreviations) is fairly new with only a few studies written on it to date (D'Arcy et al. 2014; Ament & Haag 2016; Lee et al. 2016). All of these studies have found that security-related stress does indeed exist in organizations and is one of the roots for noncompliance issues. Additionally, all of these studies have studied the phenomenon of SRS quantitatively through questionnaires, which leaves the research gap of qualitative research on SRS to be filled.

It is largely agreed upon by all of the previous SRS research that the topic needs to be further studied. Lee et al. (2016) state that their study should be used as a cornerstone for future information security stress research, and suggest future research on organizational factors mitigating SRS as well as the management side of the phenomenon. Ament & Haag (2016) point out that their research is a "first test of the security-related stress construct" and that further research on the topic is needed to find out how stress affects other areas than just information security policy (ISP) compliance, for example individual productivity, performance or job satisfaction. Ament & Haag (2016) also suggest future research on the link between SRS and technostress, and state that a more objective study that focuses on a single organization is needed, since their own sample was very broad and the data collected was based on the subjects' own perceptions as they answered the questionnaire. D'Arcy et al. (2014) also suggest a more objective approach to future research as it may reveal new insights and supporting details to the already discovered results.

This thesis will be addressing the research gap by approaching the phenomenon with a qualitative study using interviews. As all previous research has been done through questionnaires, it is important to understand the phenomenon more broadly through qualitative research. By studying the phenomenon of SRS through interviews, the result will be a deeper and more thorough understanding of end-users' attitudes and concerns towards stressful information security practices. This thesis will answer to the future research need expressed by both Ament & Haag (2016) and D'Arcy et al. (2014) of a more objective study focusing on a single organization. The interviews could also reveal some new aspects of SRS that have yet to be discovered.

1.3 Research questions

This research is focused around three research questions which will be answered through a literature review and an empirical study. The research questions, which have been designed to answer the main question of how organizations can improve their information security practices to reduce SRS, are as follows:

1. What do technostress and security-related stress have in common?
2. Why and how do employees experience security-related stress?
3. How can organizations improve their information security practices to prevent and reduce security-related stress?

1.4 Scope of the study

The interviews will be conducted with employees from the University of Turku. The scope is limited to a single organization, as previous research on SRS has identified the need for a more controlled sample of subjects (Ament & Haag 2016). Additionally, the focus will be on employees who are end-users of the information security policy within the organization, not the security experts. The information security experts will be excluded from the scope of this study, because the aim of the study is to find out how information policies and practices affect the employees and therefore the organization.

2 TECHNOSTRESS

In order to explore the phenomenon of security-related stress, it is important to first understand the underlying concept of technostress. In the first scientific paper on technostress (Brod 1982) the concept is defined as stress arising from the inability to handle new technologies introduced to the workplace. Another early definition of technostress by Caro & Sethi (1986) defines technostress as uncertainty caused by the need to adapt to technological change, and therefore focuses more on the perceptions of inability rather than reactions to not being able to handle the technologies. While technostress can still today be considered as stress from having to adapt to and being anxious about new technologies, the phenomenon has gotten new depths as technology has become a standard tool for everyday work used ubiquitously throughout the organization (Tak & Park 2016). This chapter will review the existing literature on technostress, divided into two sections. The first part will present the causes and consequences of technostress both at the individual and at the organizational level, and the second part of the chapter will present possible ways of combatting technostress in organizations.

2.1 Technostress: causes and consequences

Numerous studies on technostress have been conducted with both a broad scope as being examined in the workplace in general (ie. Tarafdar et al. 2007; Ragu-Nathan et al. 2008), and from a more specific point of view with a focus on specific professions such as teleworkers (Suh & Lee 2017) and librarians (Ahmad et al. 2012), or on different areas of technology, such as mobile phones (Hung et al. 2011) or social media (Brooks & Califf 2017). According to Ragu-Nathan et al. (2008), technostress as a modern phenomenon can be attributed to three characteristics of the contemporary work environment depicted in Figure 1. First of all, employees are becoming more and more dependent on the constantly developing technologies to make decisions. Second of all, there is a knowledge gap between the existing competencies of end-users and the competencies needed to operate the new, increasingly sophisticated information and communication technologies. The third contributing characteristic is the shift from traditional working conventions to modern, more flexible ways of working (virtual teams, remote work etc.).

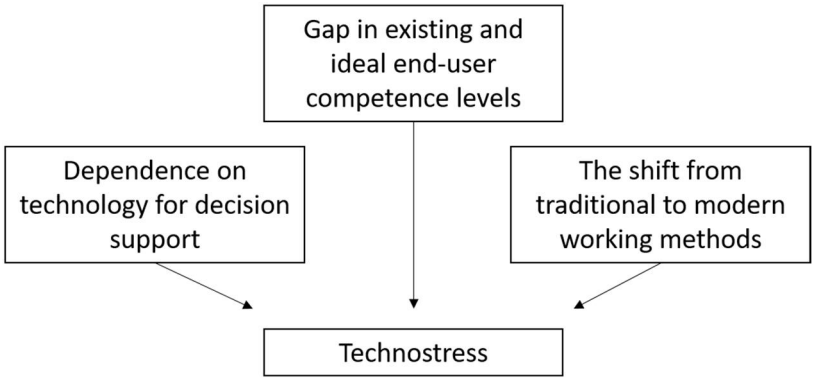

Figure 1 Three characteristics of the modern workplace contributing to the existence of technostress (Ragu-Nathan et al. 2008)

2.1.1 The five technostress creators

In their research, Tarafdar et al. (2007) identify five factors as the main creators of technostress in end-users. These five factors – techno-overload, techno-invasion, techno-complexity, techno-insecurity and techno-uncertainty – have been widely accepted in technostress literature, and have thus become the cornerstone of empirical technostress research (ie. Ragu-Nathan et al. 2008; Hung et al. 2011; Shu et al. 2011; Fuglseth & Sorebo 2014; Sellberg & Susi 2014; Srivastava et al. 2015; Fischer & Riedl 2015). Techno-overload is related to the change in end-users' working pace, namely the expectation to work faster because technology makes it possible. Techno-invasion describes the stress that arises from constant connectivity enabled by ICTs and the feeling of responsibility to be connected at all times. Techno-complexity refers to the insecurity created by sophisticated systems, which make end-users feel incompetent. Techno-insecurity is the fear of job loss due to automation or more techno-savvy workforce. Techno-uncertainty comes from the knowledge that ICTs are constantly developing and therefore end-users' own skills can become obsolete. (Tarafdar et al. 2007.)

Even though a large portion of technostress literature is based on the classification by Tarafdar et al. (2007), other theories and stressors have also been found. Ayyagari et al. (2011), for instance, take a different approach to the classification of technostress creators. They study the effects of specific technology characteristics, such as constant connectivity and the dynamic fast-changing nature of technology, on five different technostress creators which they have dubbed work overload, role ambiguity, job insecurity, work-home conflict and invasion of privacy. While the names of the stressors are to some extent different, similarities in their definitions can be found and will be explored in the following chapters. Fischer & Riedl (2015) add to the list of technostressors by Tarafdar

et al. (2007) with techno-unreliability, meaning the instability that comes from systems malfunctioning, breaking down and lagging, which leads to employees not being able to fully rely on the technologies they use. According to Shu et al. (2011), technology dependence – which refers to the degree to which end-users are dependent on computer technologies to finish their tasks – can also increase technostress.

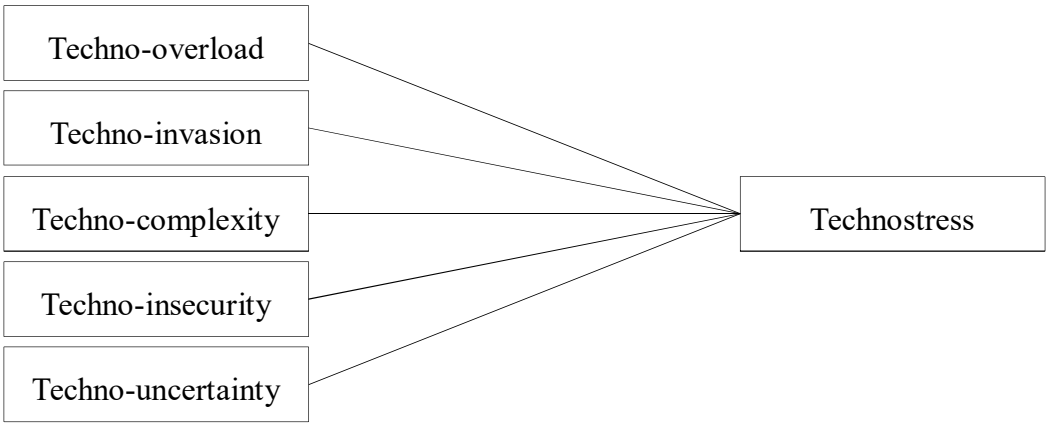

Figure 2 The five technostress creators identified by Tarafdar et al. (2007)

Being the most widely used basis for technostress (and consequently security-related stress) research, the classification of stressors by Tarafdar et al. (2007) depicted in Figure 2 will also be used for the purposes of this thesis. Techno-overload is the result of employees simply having too much to handle due to technology – be it too much work, too much information or too many simultaneous tasks (Tarafdar et al. 2007). Information systems can cause situations wherein employees are, for example, forced to work much faster as they are expected to accomplish more in less time with the help of the technologies, or are given more work than they can efficiently handle (Shu et al. 2011). Another reason for techno-overload could be the fact that end-users have to spend a significant time adapting to or learning new information systems, which takes up time from their actual tasks and leads to overload (Tarafdar et al. 2011). Ragu-Nathan et al. (2008) point to the constant stream of never-ending information as the main creator of techno-overload. Users are continuously multitasking and trying to handle information from various sources, which often results in inefficiency (Young, 2004). The need to multitask creates stress in end-users, as they are exposed to more information than they can productively process. In addition, technology can cause addiction: for instance the use of mobile applications can become compulsive, meaning that a user checks their phone many times a day for no reason, and lead to technostress (Hsiao 2016). The vast amounts of information also lead to end-users not knowing what to prioritize anymore. Ayyagari et al. (2011) also point out that a major factor causing techno-overload is the frequency at which new technologies and information systems are introduced to organizations today. Employees get

tired of having to constantly adapt to the fast pace of change in the field of technology and of having to change the way they work, and may start perceiving the new systems in a negative fashion instead of seeing the opportunities that lie within them. This is especially true with technologies that exceed the skill-levels of employees.

Techno-invasion occurs due to the fact that technology enables users to be constantly connected, blurring the line between work life and personal life (Tak & Park 2016). The constant connectivity that is enabled by new technologies leads to end-users feeling as though they are always at work (Hung et al. 2011). Knowing that it would be easily possible to read and answer e-mails during holidays or evenings makes employees feel as though they should be doing so, and can even be experienced by employees as an invasion of their privacy (Ayyagari et al. 2011). Technology is therefore invading users' personal lives (Tarafdar et al. 2011). Tak & Park (2016) call employees who are faced with such issues "connected smart workers". Ayyagari et al. (2011) identify another stressor closely related to techno-invasion called work-home conflict – referred to as work-life conflict by Tak & Park (2016) – which stems from the increasingly common practice of working from home. As employees are able and at times even encouraged to work remotely, a clear distinction between work life and home life ceases to exist. This might result in there being no end to the working day on days when work is done remotely, or in turn work continuing at home on days spent at the office, creating so called ubiquitous technostress (Hung et al. 2011). Going even further, techno-invasion can also result from the social pressure that is caused by the connectivity (Booker et al. 2014). The perception that colleagues are constantly checking their emails in the evenings for instance causes anxiety in employees.

According to Tarafdar et al. (2007), the increasing complexity of technologies that are being developed can lead to anxiety in end-users. An employee may feel inadequate and incompetent simply due to the inherent complexity of the technology (Ahmad et al. 2011; Fuglseth & Sorebo 2014). Complex technology usually comes with a set of complex jargon, which end-users may find intimidating (Chandra et al. 2015). While many companies provide supporting documents such as manuals or other study materials to end-users to aid them in understanding the systems, these materials are often not designed with the end-user in mind, and end up being too complex and too lengthy. This in turn may make the user feel even more stressed out than before reading them (Ragu-Nathan et al. 2008). Brod (1982) states that end-users may experience low self-confidence regarding their skills and jealousy over other users who seem to have a better grasp on the technology. All of this leads to the inability to solve problems with the new technologies. Tarafdar et al. (2011) note that techno-complexity is also closely linked to techno-overload, because when end-users have to spend vast amounts of their time trying to learn and understand how to efficiently use systems they find complex, it takes time away from their actual work, increasing their workload.

Techno-insecurity is defined in technostress literature as either the fear of technology changing the job market and therefore threatening the job security of employees (Fuglseth & Sorebo 2014), or as arising in end-users when they feel threatened by the skills of their coworkers, who they feel have a better grasp of the technology (Ahmad et al. 2011; Chandra et al. 2015). Living under constant fear of being replaced by someone or something more competent is stressful, and may lead to employees pretending to possess skills they don't have (Tarafdar et al. 2007). According to Spacey et al., (2003) ever since the dawn of the new technological era, news about robots and technology stealing jobs has caused workers to feel discomfort as they contemplate whether their job will be safe in the future. Techno-insecurity may create a vicious loop in an organization, as employees keep information from their peers and refuse to share their skills out of fear of becoming obsolete as their co-workers learn the same things (Tarafdar et al 2011).

Techno-uncertainty occurs as employees are under pressure to keep up with the latest technologies, when there is no way of knowing when they have to move on to a new system again (Tarafdar et al. 2007). Employees are constantly being introduced to new technologies, which leads to a loss in stability in working patterns. Fuglseth & Sorebo (2014) add that techno-uncertainty can also arise from having to face constant upgrades of original software and hardware. This, according to Ragu-Nathan et al. (2008) creates uncertainty in end-users, because it generates ambiguity in current job demands and makes the future job demands unpredictable. Chandra et al. (2015) find that the short life-cycles of today's technological commodities cause frustration in employees as their skills regarding any certain technology may become obsolete at any time. Ayyagari et al. (2011) identify another ambiguity stressor called "role ambiguity", which can be considered a cross between techno-overload and techno-uncertainty. Role ambiguity arises from having to multitask with different systems and tasks, and not knowing what to prioritize. Trying to focus on a job task and being constantly interrupted by e-mail notifications or phone calls on other topics can lead to not knowing which task is the most important. The problem is getting more serious as the sources of interruption in the workplace are increasing and the workforce is getting older and more sensitive to such interruptions (Tams 2011).

2.1.2 Consequences of technostress on individuals and organizations

Fischer & Riedl (2015) find it ironical that while ICTs are usually introduced to decrease stress in employees by automating and making work easier and faster, through technostress they end up having the opposite effect. This is in information systems literature often referred to as the "dark side of ICT" (Tarafdar et al. 2011; Fischer & Riedl 2015; Srivastava et al. 2015; Salah-Eddine & Bleaissaoui 2016). Technostress has been found

to have a variety of different consequences at both the employee and the organizational level (Hung et al. 2011; Okebaram & Moses 2013).

Fischer & Riedl (2015) attribute technostress experienced by employees to five antecedents, which represent the present state of the organization: individual characteristics, job characteristics, the technological environment, the organizational environment and the social environment. As agreed by other researchers (ie. Shu et al. 2011; Ragu-Nathan et al. 2008), individual characteristics such as age, personality or subjective perceptions of situations that are affected by a lack of information have a major influence on technostress experiences. Job characteristics, which determine how difficult or demanding an employee's tasks are, are another determinant of technostress (Suh & Lee 2017). The technological environment includes the technologies that have been adopted to an organization and how they are managed, including how often they are changed or how reliable their use is. The organizational environment refers to the physical and organizational atmosphere (layout of the office, company culture and level of technical support) of the company and the social environment to the atmosphere that is created in social interactions. (Fischer & Riedl 2015.) Brooks & Califf (2017) study the effect of social media use at work, and find that employees using social media during working hours is detrimental to productivity due to social media induced technostress impacting the mental wellbeing of employees. According to the researchers, this interesting finding also speaks to the fact that as technology is changing, organizations are no longer just responsible for making sure that technostress from their own technologies is in control, but also taking into consideration technologies that the company doesn't provision to the employees.

When it comes to individual characteristics, Brod (1982) states that prior experiences with technology and how in control end-users are of technology largely determines whether or not they will experience stress due to technology. Srivastava et al. (2015) find that personality traits, such as an employee's level of neuroticism or extraversion affect exposure and reactivity to technostress. Ragu-Nathan et al. (2008) study the effect of four individual characteristics – age, gender, education, and computer confidence – on whether or not a person will experience technostress. They find that as education and computer confidence increases, users become less inclined to experience technostress. However, their initial assumptions about age not being a factor and women being more inclined to experience technostress than men is proven wrong. Their study reveals that technostress actually decreases as users get older, and that males experience more technostress than females. In respect to the surprising finding about age, Ragu-Nathan et al. (2008) propose that older professionals have better stress-management skills and more power over the choice of using information systems in the workplace and therefore are less prone to experiencing technostress. Tams' (2011) findings are in contradiction with this conclusion, as they suggest that older generations are more sensitive to interruptions, and consequently technostress arising from interruptions does increase with age. Regarding gender

differences, Ragu-Nathan et al (2008) suggest that a possible explanation could be the fact that women use less information systems in their work roles than men. Viswanath & Morris (2000) find that when choosing technologies and systems, women are more likely to focus on ease of use while men make their decision based on their perceptions on how useful the technology will be. This is in line with Tarafdar et al's (2011) finding, as technologies that are easier to use cause less techno-overload and techno-complexity.

Tarafdar et al. (2011) classify the individual consequences of technostress into two categories, the psychological and the information system use related outcomes. Psychological outcomes include decreased end-user job satisfaction and decreased end-user commitment, as well as increased role conflict and increased role overload. Job satisfaction decreases as end-users keep experiencing and trying to handle technostress at the workplace. Tak & Park (2016) find that technostress mostly affects job satisfaction indirectly through work-life conflict, which refers to the constant connectivity enabled by technologies. The negative feelings that arise are linked to the organization, even though they are outcomes of frustration towards technology, and thus a decrease job satisfaction. According to Ragu-Nathan et al. (2008) the biggest organizational consequence of technostress is that it leads to a decrease in employees' commitment to the organization and to their intention to stay, however differing opinions exist as well. For instance, Ahmad et al. (2012) find no correlation between the two phenomena. Role conflict refers to end-users experiencing contradicting requirements in their work (Okebaram & Moses 2013), and technostress increases role conflict by creating situations where these contradictions become more apparent (Tarafdar et al. 2011). Role overload, which refers to having too many tasks or tasks that are too difficult in comparison to the expectations and the skills of the employee, is increased in employees who are stressed due to technology (Wang & Shu 2008).

The information systems use related outcomes of technostress include decreased user satisfaction with specific information systems, decreased user productivity when using systems, and decreased user innovation in the use of systems (Tarafdar et al. 2011). User satisfaction with information systems decreases for instance when users don't know how to best benefit from systems, when systems crash or when data is lost. Owusu-Ansah et al. (2016) study the effects of technostress on commercial banks and find that employees are experiencing anxiety and have a very negative attitude towards information systems at their use. The results also show that technostress causes decreased performance as the banking professionals are having trouble adapting to the fast-paced technological change, and that having to constantly learn new systems and spending time trying to solve mistakes that come from not being familiar with a system decreases end-user productivity. This finding is in line with a study by Tarafdar et al. (2010), where end-user satisfaction in the context of technostress is also proven to depend on how positive end-users' perceptions are towards the technologies they use in their daily work. Innovation, meaning

experimentation and coming up with new and exciting ways of making use of information systems, is decreased when end-users are experiencing technostress (Fuglseth & Sorebo 2014).

Ahmad et al. (2012) emphasize that the effects of individual consequences of technostress directly also affect the organizational consequences of technostress, as happy employees are more committed to the organization. At the organizational level, technostress can be manifested as absenteeism, conflicts between employees, overall employee dissatisfaction and disloyalty towards the organization, all of which can be detrimental to organizational productivity (Caro & Sethi 1986). Suh & Lee (2017) find that there's a direct link between how employees at a teleworking company experience technostress and how valuable they are to the organization in terms of productivity. Work overload, invasion of privacy and role ambiguity along with the fast pace of technological pace are proven to decrease the teleworkers' satisfaction. Hung et al. (2011) study ubiquitous technostress, meaning stress that is caused by the universal presence of technology in organizations, and find that not only does such stress exist, but that through increasing role stress, ubiquitous stress also has a negative effect on productivity.

As is the case with individual consequences, organizational consequences can also vary depending on what kind of organization is in question. Tarafdar et al. (2015) study technostress in the context of sales professionals, and find that technostress creators negatively affect sales performance and technology-enabled innovation. They show that, for example, techno-overload experienced by sales professionals when having to input customer information into a sales support system or a CRM system takes up valuable time from the actual selling, hence leading to a loss in performance. Sales employees could also feel inadequacy due to techno-insecurity, which leads to anxiety towards the systems and prevents the sales professionals from being innovative in their work.

It is important to keep in mind that technostress can also have positive consequences in the organization, in the form of technoeustress (Ahmad et al. 2012). End-users perceive technostress creators in the workplace in different ways, which – depending on users' personality traits – leads to either distress or eustress. Organizations could leverage the fact that personality traits have an influence on how employees react to technostress creators as either distress or eustress. Giving complex and jobs to employees who perceive challenges as opportunities rather than as stressful events will decrease technostress in the organization (Srivastava et al. 2015). Managers can keep this in mind already when drafting job descriptions for example.

2.2 Ways of combating technostress

After exploring the consequences technostress has at both the individual and the organizational level, it is clear that something needs to be done to prevent technostress from manifesting itself in an organization. Technostress literature has identified so-called inhibitors which act as moderating tools to reduce technostress experienced by employees (Young 2004; Ayyagari et al. 2011; Fuglseth & Sorebo 2014; Srivastava et al. 2015; Pirkkalainen et al. 2017). Figure 3 showcases the most common inhibitors of technostress mentioned in research, which are continuous training, technical support provision, user involvement facilitation, supporting end-user innovation and systematically managing technostress. Caro & Sethi (1986) emphasize the high importance of top management support for all methods of technostress management.

Top management support			
Continuous Training	Technical support provision	User involvement facilitation	Innovation support

Figure 3 Ways of combating technostress

Perhaps the most widely accepted suggestion in technostress literature to prevent and control technostress is to provide continuous training on the systems and technologies that end-users find stressful (ie. Spacey et al. 2003; Hung et al. 2011; Fuglseth & Sorebo 2014). According to Spacey et al. (2003), training becomes successful when it is tailored to the needs of the employees, keeping in mind that different types of needs may appear in different groups of employees. Tarafdar et al. (2011) state that providing training and supporting documents for system use increases users' system skills, which in turn directly reduces techno-overload, techno-complexity and techno-insecurity which are mainly caused by not understanding the systems. Spacey et al. (2003) stress the importance of continuous training, instead of occasional one-time training sessions, to make sure that end-users feel confident about their skills in the long run and acknowledge why new systems are implemented. The knowledge that training is always available and that it is a key value of a company also helps with techno-uncertainty, because employees feel as though they will be supported in situations where new technologies are introduced. Techno-invasion could be prevented by setting clear guidelines to when users should be answering e-mails for example, and training users on the company human resources policies where these guidelines are explained. A recent example of such a policy is the "right to disconnect" that was enforced by the French government in 2017, which obliges all companies with over fifty employees to draft into their code of conduct a clear rule against sending e-mails during out-of-office hours (bbc.com 2016). Spacey et al (2003) note that while

training is one of the best methods in influencing end users and helping reduce technostress, poor training can have the opposite effect of what is the desired outcome. According to the researcher, having an inadequate trainer may even induce technostress as users either get the feeling that the technology is even too complex to master by a professional or that they don't have support available. As noted by Okebaram & Moses (2013) training might also be perceived by the employees as overloading, if it doesn't occur at a convenient time or if it takes away from productive working time. Hung et al. (2011) support the idea of not only training employees on technical capabilities but also on coping with technostress, as their results showed that for instance ubiquitous technostress can be addressed through training on employees on overall stress management, because technostress can be closely related to role stress.

Technical support provision, especially easily approachable and supportive helpdesks, can have a significant effect on reducing technostress, because it lessens the burden of end-users to have to solve problems by themselves (Fuglseth & Sorebo 2014). If it is made easy for an end-user to ask and get answers for their technical issues with the systems, it dramatically decreases the anxiety and stress that is caused by the systems. Users no longer feel as though they have to spend significant amounts of time figuring out how to solve problems on their own, and can therefore focus more on their own work. Users are also less inclined to make dramatic mistakes if they know help is easily available (Tarafdar et al. 2011). According to Tarafdar et al. (2015) organizations should also make sure that the organizational environment is such that promotes support. Sellberg & Susi (2013) point out that support needs to be something that is available constantly, and give as an example organizations where employees are working (and expected to use technology) around the clock, but technical support provision is only available during normal office hours. Salanova et al. (2013) find, that in addition to technical support, negative effects of technostress can also be counterfeited by social support from colleagues or managers. A good environment makes users feel comfortable asking for advice and assures that there is no stigma in needing to ask for help. The negative perceptions of having to constantly keep oneself up to date with new technologies are lessened when end-users know that there is effective support available whenever new systems are introduced. (Salanova et al. 2013.)

User involvement facilitation means giving end-users the chance to participate and be involved in the planning, development and implementation of new technologies into an organization, already defined as a necessary step in ICT implementation in the 90s (Blili et al. 1998; Clark & Kalin 1996). Technostress decreases as users are familiarized with systems prior to using them (Hung et al. 2011). By being involved in the adoption process of new technologies, end-users are less likely to feel that the new technologies cause disruptions in their work as they are aware of the implementation schedule and reasons for the introduction of the systems (Spacey et al. 2003). Okebaram & Moses (2013) give the

example of not including bank workers in the automatization of bank processes in the 70s and 80s, describing it as a major mistake because it distanced the workers from the technologies right from the beginning. First of all, such distancing could have been avoided through involvement facilitation, as users would have been able to get more familiar with the systems from the get-go, giving them confidence in using the systems and making the new technologies feel less complex. Secondly, by involving users in the introduction of a new system, users are able to express what they need from the system and see how this corresponds to what the system can offer. When the requirements are clear, users don't need to spend an excessive amount of time figuring out what the system can be used for but instead find the system useful and informative. Thirdly, the involvement mechanisms help end-users know what is going to change in the work environment through the introduction of the new ICTs, giving them the feeling of control over the change. The perception of control in coping with technostress is also discussed by Pirkkalainen et al. (2017), who find that so-called "IT-control", meaning the level of control an end user has over using a certain technology, can help mitigate the negative consequences of technostress because users feel that it is their choice to use the system. This also helps users plan ahead and predict the changes that are about to come, and decreasing uncertainty. Wang & Shu (2008) suggest that perceived organizational support – meaning how much the employee believes he or she is given support if need comes – helps in alleviating technostress. This is an interesting finding, because it speaks to the effect the work environment's ambiance can have on an individual.

Salo et al. (2017) emphasize "that IT users should not be depicted as helpless sufferers of technostress whose mitigation depends solely on external or organizational mechanisms", but that employees can themselves have an effect on how they experience stress. The researchers present three mitigation types, including stressor reduction (transforming old habits that cause stress), stressor toleration (transforming the way in which the employee personally reacts to the stressor) and recovery from strain (going offline). A similar idea is behind innovation support, where change management is facilitated, because introducing new technologies to an organization also means introducing new working methods to end-users (Tarafdar et al. 2010). In a parallel way, Young (2004) states that the key to reducing technostress is to find the balance between how technology can be consumed and how it consumes the user. In helping to find a balance in dealing with technostress, users should be aware of which aspects of technology are stressful. Users can then start focusing on the problem areas. For instance, if an employee notices that technology-enabled multitasking is something that is creating stressful situations in their work, they should pay attention to slowing down and focusing on one thing at a time. Having end-users innovate ways which would help them learn and adapt to the new ways of working more efficiently reduces stress that would otherwise arise from the changes.

Organizations should provide an organizational environment that encourages experimentation. By encouraging end-users to explore the systems and innovate new ways of using the systems, users are able to learn how to use the systems at a deeper level, which lessens the insecurity they feel towards the technology. (Tarafdar et al. 2011.)

Finally, reducing technostress in organizations requires support from management in order to be successful (Caro & Sethi 1986). Okebaram & Moses (2013) state that since the antecedents of technostress often come from organization-wide developments, such as introducing new technologies or changing the working environment by automatizing something, the management of the changes is extremely important. All the inhibiting factors of technostress – from training to technical support and from to involvement facilitation innovation support – are either unenforceable or ineffective if top management is not invested in making them successful.

Table 1 ties together the research findings on creators and consequences of technostress along with ways of combatting the negative consequences of the phenomenon. The following chapter presents the findings from similar aspects on security-related stress, which are summarized in Table 2 to facilitate answering the first research question of what technostress and security-related stress have in common.

Technostress	Aspects	Researchers
Creators	Techno-overload Techno-invasion Techno-complexity Techno-insecurity Techno-uncertainty	Spacey et al. 2003; Young 2004; Tarafdar et al. 2007; Ragu-Nathan et al. 2008; Hung et al. 2011; Hsiao 2016; Tarafdar et al. 2011; Shu et al. 2011; Ayyagari et al. 2011; Tams 2011; Ahmad et al. 2011; Fuglseth & Sorebo 2014; Sellberg & Susi 2014; Chandra et al. 2015; Srivastava et al 2015; Fischer & Riedl 2015; Tak & Park 2016
Conse-quences	**Employee-related** Decreased job satisfaction Decreased commitment Increased role conflict Increased role overload Decreased system-related satisfac-tion Decreased productivity Decreased user innovation	Wang & Shu 2008; Ragu-Nathan et al. 2008; Tarafdar et al. 2011; Okebaram & Moses 2013; Fuglseth & Sorebo 2014; Tak & Park 2016; Owushu-Ansah et al. 2016
	Organizational Absenteeism Conflicts between employees Overall employee dissatisfaction Disloyalty towards the organization Lower productivity	Caro & Sethi 1986; Hung et al. 2011; Ahmad et al. 2012; Tarafdar et al. 2015; Srivastava et al. 2015; Suh & Lee 2017
Ways to combat	Continuous training Technical support provision User involvement facilitation Innovation support Top management support	Caro & Sethi 1986; Clark & Kalin 1996; Blili et al. 1998; Spacey et al. 2003; Young 2004; Wang & Shu 2008; Tarafdar et al. 2010; Hung et al. 2011; Ayyagari et al. 2011; Tarafdar et al. 2011; Okebaram & Moses 2013; Sa-lanova et al. 2013; Fuglseth & Sorebo 2014; Sellberg & Susi 2015; Tarafdar et al. 2015; Srivastava et al. 2015; Pirk-kalainen et al. 2017; Salo et al. 2017

Table 1 **Summary of causes, consequences and remedies for technostress in scientific literature**

3 SECURITY-RELATED STRESS

Cybersecurity is getting more attention than ever before, with widespread ransomware attacks bringing the operations of organizations to a halt, presidential elections being tampered with and governmental classified information being stolen by hackers (Cate et al. 2017). According to Gartner's (2017) predictions, the global year-over-year growth of information security spending will be 7% ($86,4 billion) in the year 2017 and up to 7,6% more ($93 billion) the following year. Information security is an actual and growing threat in organizations worldwide. Companies are using considerable amounts of money to secure their data, but at the same time the employee – who is often considered as the weakest link of the organization (Angermeier et al. 2009; Aurigemma 2013) – is neglected in the process. The poor implementation of information security practices to the organization has brought rise to a new field of technostress research, so-called security-related stress (SRS) (D'Arcy et al. 2014; Lee et al. 2016; Ament & Haag 2016). This chapter will introduce the concept of SRS by reviewing the scarce amount of previous research on the topic (D'Arcy et al. 2014; Lee et al. 2016; Ament & Haag 2016) combined with related stress and information security research in the field of information systems.

3.1 A conceptualized model of security-related stress

SRS in the field of ISS can be defined as employees' stressful reactions to information security practices, requirements and incidents (Ament & Haag 2016). An example of a situation where information security can result in stress is when an employee finds the information security policy (ISP) filled with jargon, time consuming to go through or too difficult to understand. Similarly, SRS can be the result of an employee hearing disconcerting news about security breaches or data loss from the media. In their conceptualized model of SRS, Ament & Haag (2016) identify six stressors causing security-related stress in three different environments (Figure 4). The work environment causes SRS in the form of complexity, overload and uncertainty. Invasion of privacy is a stressor in the personal environment, and conflict and news are security-related stressors in the social environment of an employee.

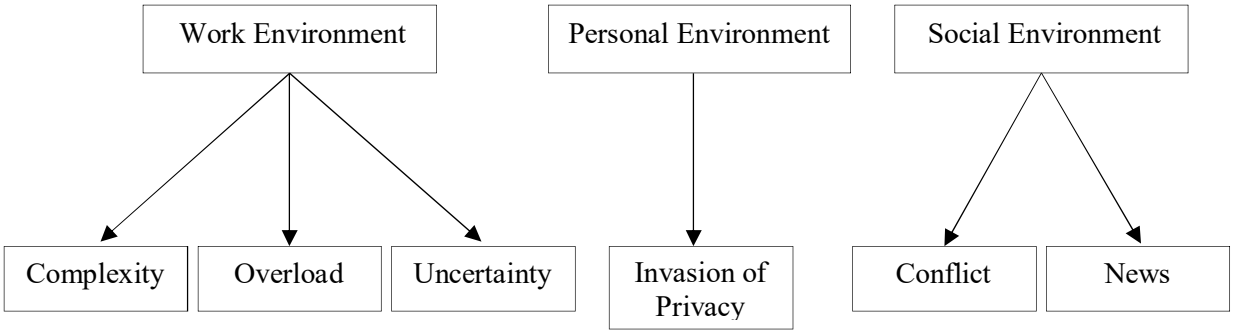

Figure 4 A Conceptualization of SRS used by Ament & Haag (2016)

3.1.1 Security-related stress and the work environment

Security-related stress in the work environment can be attributed to three different stressors – already familiar from technostress research (Tarafdar et al. 2007), but with different definitions for SRS – which are complexity, overload and uncertainty experienced by employees in the context of information security (Ament & Haag 2016). SRS can arise from both the managerial and the technical information security efforts of the organization (Lee et al. 2016). Managerial information security consists of creating information security processes and policies and improving security behavior, while technical information security consists of technical security measures, restrictions and applications.

D'Arcy et al. (2014) define SRS complexity as stress that arises from information security requirements being too difficult to understand or to comply with, causing the employee to either have to invest significant amounts of time in trying to understand the requirements or to have to guess which is the right course of action. An example of a situation where an employee might experience stress due to the complexity of a requirement is one where he or she has to check the policy to make sure they are not violating any rules, but finding it filled with technical content or jargon. Stahl et al. (2012) study information security policies in the UK healthcare sector, and find that indeed there are significant amounts of jargon and ambiguity in the policies, making it unlikely for employees to have a consistent and clear understanding of what is expected of them. The jargon in the policies is very technical and clearly not written with the healthcare professional in mind. Such requirements, which are hard to understand and may be interpreted in many ways, can according to D'Arcy et al. (2014) result in employees having to spend a long time in finding what they are looking for or simply not understanding how to act. Ament & Haag (2016) give the example of an employee having to connect to the company's private network from outside the organization but not knowing how to do so due

to complex steps that are not explained clearly enough. SRS complexity can cause involuntary security breaches by employees who would want to comply but do not know how to, according to Guo (2013) so-called "non-malicious security violation".

D'Arcy et al. (2014) define SRS overload as the result of information security requirements causing extra workload for employees and taking time away from their actual work. According to Herath & Rao (2009), employees may also decide to ignore the information security policy – not solely because it adds to their workload – but also because it's more convenient to act in another way. Ament & Haag (2016) find in their research that password management in the modern-day work environment is the most significant cause of SRS overload, as employees are constantly forced to think of, remember and update different passwords for different systems. Hedström et al. (2011) find that while often the information security practices of an organization are built and communicated in a control-based top-down manner, they should rather be built using a value-based approach which considers the values of the employee in the information security guidelines. The researchers use the healthcare sector as an example, where often the number one values of the employees concern the patient's health, which sometimes leads to the healthcare professional breaking information security guidelines by prioritizing fast treatment. If the values of the healthcare professional were taken into consideration in the information security policy and requirements, and the use of secure passwords for instance would be explained through the safety of the patient, the message in the information security policy would become easier to resonate with. Another example of an information security requirement causing overload are preset access restrictions in a system, which require having to always go through a helpdesk or someone who has administrative rights to a system to get work done (Ament & Haag 2016). Similar loss in productivity is caused by automatic system updates which might catch the employee by surprise mid-task causing loss of work or loss of time in case the update is lengthy, or simply interrupt the employee's workflow (D'Arcy et al. 2014).

Interruptions in workflow caused by information systems or technology in general have been proven to lead to lower quality decision-making and negative attitudes towards the causes of interruption, ultimately causing stress in end users (Speier et al. 1997). Work overload results especially from technical security requirements (Lee et al. 2016). Technical security requirements – as opposed to managerial security requirements – are technical security protocols, such as administrative limitations and data restrictions that can take away considerable time from actual work. Lee et al. (2016) suggest that technical security measures, while often inevitable for an organization – should be adopted gradually in order to prevent work overload. Often when a new technology or system is introduced to an organization, it brings along new security protocols and rules to follow, and if they are all introduced at one go, they might feel overwhelming. The constant adoption of new security measures may lead to so-called compliance burn-out (El-Den et al. 2014),

meaning employees – even those who are morally engaged to follow guidelines – getting exhausted of having too many requirements to learn and comply with.

The third stressor of the work environment – SRS uncertainty – refers to the stress caused by the fast-paced development of the information security environment and therefore requirements (D'Arcy et al. 2014; Ament & Haag 2016). Employees are expected to keep themselves up to date on the information security requirements of the organization, but this task becomes more and more difficult as constant technological development, changes in legislation around information security, and the adoption of new systems forces the organization to constantly revamp existing requirements. A good present-day example of a stressful information security update, that has already caused a lot of uncertainty before even being implemented, is the General Data Protection Regulation (GDPR) enforced by the European Union coming into effect in May 2018 (Murtaugh 2017; Albrecht 2016). According to Gartner (2017), the new regulation has caused panic in European and multinational organizations alike, reflected in the fact that up to 65% of all information security spending decisions are driven by the GDPR. The new regulation causes many changes and updates, affecting all companies that collect or use data, and the consequences of not implementing those changes to the organization's information security policy and further into the work routines of employees can have severe monetary consequences: the sanctions are up to 20 million euros or 4% of the annual turnover of an enterprise (Hoyle 2017).

3.1.2 Security-related stress and the personal environment

In the context of technostress, Tarafdar et al. (2007) identified techno-invasion as the result of technology enabling users to be constantly connected, and blurring the line between work life and personal life. The constant connectivity that is enabled by new technologies leads to end-users feeling like they are always at work. The feeling of knowing that it would be easily possible to read and answer e-mails during holidays or evenings makes end-users feel as though they should be constantly available. This leads to technology invading users' personal lives (Tarafdar et al. 2011). Invasion of privacy as a stressor in the information security context is linked to employees' concerns about being monitored and having their privacy violated (Lee et al. 2016), which is in fact more in line with the definition of techno-invasion by Ayyagari et al. (2011) from technostress research, as Ayyagari et al. also see techno-invasion as stress that comes from an end user feeling as though their privacy is being violated by technology. Employees are concerned that their information security behavior – and overall behavior on the Internet and in different communication technologies at work – is being monitored without their knowledge (Ament & Haag 2016).

According to Lee et al. (2016) information security measures place too much focus on monitoring employees' information security practices and compliance activities, leading employees to feel that their privacy is being invaded. The researchers suggest a selective and targeted approach to information security compliance monitoring. This means that organizations should take a different approach to monitoring employees with different levels of access to systems and data. The reasoning behind selective monitoring is that if employees are all monitored in the same way regardless of their job roles, then the practice of monitoring seems random and unrelated to the actual end result of wanting to secure data and information assets of the organization. An employee who is working in human resources and has access to all employee data should be monitored on a different level than an employee who doesn't have any access to employee or customer data. With the former, the closer monitoring of information security compliance is justified, whereas with if the latter is still monitored in the same fashion may feel that it is unnecessary and invasive (Lee et al. 2016). Ament & Haag (2016) go as far as to suggest that if employees are well trained on information security practices, they won't need to be monitored at all.

Ament & Haag (2016) theorize that two additional stressors in the personal environment – job insecurity and degree of freedom (not represented in the conceptualization in Figure 4) – could be contributing factors to security-related stress. Job insecurity as theorized by Ament & Haag means employees fearing job loss due to insufficient information security skills. Degree of freedom, both in the sense of not having enough freedom or having too much freedom in decision making regarding information security is suggested as a contributor of SRS. A situation where information security limits the degree of freedom is when a security requirement restricts the amount autonomy, innovation or experimentation an employee can do in their work. On the other hand, if the employee has too much freedom and responsibility in making information security related decisions, they might feel that they aren't equipped to make such decisions and don't want to be held responsible for decisions they weren't comfortable making in the first hand. While Ament & Haag (2016) don't find adequate support for job insecurity or degree of freedom in their study, they suggest retesting both suggested stressors in the future as information security develops in organizations.

3.1.3 Security-related stress and the social environment

The research by Ament & Haag (2016) identifies and validates two stressors which have not been taken into account in technostress research, but rather can be considered distinct characteristics of security-related stress. Stress that arises from conflicts means stress that is the result of conflicting expectations employees face in their work. For instance, an organization's information security policy could mandate employees to only use internal

company communication channels when dealing with work-related information, but an employee's supervisor would ask for details on a specific work-related case through a social media channel such as Facebook or WhatsApp. This is an example of a security-related conflict, where the employee is put in the stressful situation of having to choose whether to comply with the information security policy or the supervisor's expectations. Another conflict situation could arise from stigma related to employees strictly following the information security policy.

Security-related stress can also be the result of news, such as reports about security gaps or breaches in or outside the organization (Ament & Haag 2016). In the context of SRS, "news" include any information absorbed regarding information security be it from the media, from conversations with colleagues or from social interactions outside of the work environment. Employees might for instance hear about a security gap in a system they are using at work or get news of another employee being fired due to a misuse of company data and wonder if they are themselves being compliant of the company's information security requirements. A good recent example of such news is that of the two biggest ransomware attacks in history breaking out consecutively in the summer of 2017. First in May and then in June of 2017, the two outbreaks – WannaCry and NotPetya – caused panic and uncertainty around the world (theguardian.com, Cate et al., 2017). Both ransomware attacks exploited a vulnerability in an old version of Windows, meaning that only systems that had not been updated were affected (heavy.com). An interesting finding that made by Shackelford (2017) about the two attacks was that NotPetya used the same vulnerability as WannaCry, meaning that even after as rude an awakening as WannaCry, some organizations still failed to update their systems. A possible explanation could be found from the study by Herath & Rao (2009), where the finding was that in fact, employees often tend to underestimate the chances of a security breach happening in their specific organization.

According to Anderson et al. (2016), there's a clear inconsistency in how users are worried about their information security and how they are using preventive measures or reacting to security warnings or security software updates, dubbed by the researchers as "a discrepancy between security intentions and behaviors". For instance users often ignore updates or security messages sent by security software because they have grown accustomed to these messages. This so-called "habituation to security warnings" which leads to ignoring critical information security practices/prevention measures can according to Anderson et al. (2016) be prevented by developing the user interface (UI) and user experience (UX) design of security systems. Instead of addressing the problem through time consuming trainings and information sharing sessions, the problem could be addressed by choosing information security vendors which have taken such things into consideration.

In conflict with Shackelford's (2017) and Anderson et al.'s (2016) findings regarding security behaviors, Ament & Haag (2016) find that employees who experience SRS from conflict and news are more likely to follow the information security policy and be more compliant. In theory this would mean that stressful information security practices in the form of conflict and news may enhance employees willingness to follow the company's information security policy.

3.2 Ways of combatting security-related stress

Chapter two presented training, technical support, management support, user involvement in system development and innovation involvement as methods of combatting technostress in end-users. While security-related stress literature to some extent suggests the same methods as its antecedent to combat the negative effects of SRS, a different approach needs to be taken for instance with security trainings (Ament & Haag 2016). Moreover, in addition to the aforementioned methods, SRS literature suggests the improvement of the information security policy, communicating requirements visually and recognizing security-related behaviors as field-specific reducers of SRS.

The information security policy plays an important role in combatting security-related stress. D'Arcy et al. (2014) emphasize the importance of making the information security policy as end-user friendly as possible. The first mistake designing an ISP is having it contain a myriad of technical terms or security jargon that is only understood by information security experts (D'Arcy et al 2014; Ament & Haag 2016). The vocabulary needs to be easy to follow, designed with the weakest link of the organization – the employee – in mind. Instructions on how to comply and what is expected from the side of the end user need to be made as clear and detailed as possible. El-Den et al. (2014), suggest that users shouldn't have to always refer to the information security policy when they need to check security requirements and compliance instructions. The key compliance information and most critical requirements should rather be present in the organization through educational posters or leaflets with infographics around the office. Simple wording and pictures make the message go through more effectively.

Guo (2013) presents four broad level security-related behaviors that manifest themselves in an organization. These behaviors – which organizations should strive to recognize to better understand how information security requirements are being perceived and complied with amongst employees – security assurance behavior (SAB), security compliant behavior (SCB), security risk-taking behavior (SRB) and security damaging behavior (SDB). The two first behaviors, SAB and SCB, both protect the information security of an organization, as SAB is an active and preventive form of security behavior and SCB a behavior that is in accordance with the ISP of the organization. The two latter behaviors,

(SRB and SDB) are both behaviors that are a cause for concern in the organization. Security risk-taking behavior means non-malicious but intentional breaking of the security rules, for instance taking the risk of sharing passwords or writing passwords down. Security damaging behavior is malicious and intentional behavior that is aimed at harming the organization, such as stealing company data.

According to Guo (2013), while SCB should be made into the norm in any organization as it means complying with the given requirements, the SAB activities should be rewarded and promoted. Signs of SRB and SDB need to be detected and watched out for. SDB means that an employee is purposefully harming the organization through information security misconduct, and this type of behavior should not be present in the organization. However SRB, due to the fact that it is non-malicious, is common in organizations and can be changed through education. D'Arcy et al. (2014) suggest addressing the issue of what they call "cognitive rationalization mechanisms" meaning employees justifying their own information security policy violations much like in security risk-taking behavior head on. This can be done through emphasizing that each employee has a responsibility towards securing company data, that there is no instance wherein violations can be justified, and finally that violations can result in reputational and financial consequences as well as direct consequences to employees or customers.

Promote:	**Make into the norm:**	**Detect and address:**	**Detect and eliminate:**
SAB (Security Assurance	SCB (Security Compliant Behavior)	SRB (Security Risk-taking Behavior)	SDB (Security Damaging Behavior)

Figure 5 Four information security behaviors and how to address them (Guo 2013)

As is the case with technostress, SRS can also be addressed through training (D'Arcy et al. 2014; Lee et al. 2016; Ament & Haag 2016). Employees attitudes towards information security compliance are linked to their perceptions of how much of a threat a breach in information security actually is to them (Lee et al. 2016). This is why trainings should not only focus on what not to do and how to protect the employee and the organization from security threats, but also on educating employees about the threats and their possible implications. Karjalainen & Siponen (2011) study the design of information systems security trainings, and find that a special approach should be taken when conducting information security training sessions. The widely accepted training method, suggests that information security training should consist of four phases, which are

1. Involving concrete experiences
2. Engaging reflective observation
3. Supporting formation of abstract concepts and generalizations
4. Enabling active experimentation

The first phase encourages participants to consider their own concrete experiences and attitudes towards information security practices in the company. For instance, employees can start by reflecting upon their use of passwords. An example of a concrete experience could be that an employee finds it frustrating to have to have five different passwords for different systems or for instance admit that they use the same password in all systems. After individual level reflection, the training moves on to the second phase where participants share and discuss their experiences in small groups. The discussion in the second phase is guided pedagogically by the trainer asking questions such as why are certain security and measures practices implemented into the organization and what could be the implications of not following information security protocols. Therefore instead of lecturing about the importance and reality behind information security measures in a company, participants are coming up with the reasons on their own. D'Arcy et al. (2014) support the importance of users' involvement in the design of information security requirements especially to combat SRS overload. If employees are included in the process of creating the information security policy, they're less likely to find the measures taken as a burden, but rather actually see the meaning behind these measures. In the third phase of the information security training as designed pedagogically by Karjalainen & Siponen (2011), employees' personal and collective experiences are reflected towards the actual guidance and policies of the organization. The idea is to examine the actual information security policies of the organization and see how they differ from personal or shared experiences and compliance. As a result, groups are able to identify those parts of the information security policy that clash with the reality. The final phase of the training, enabling active experimentation, aims at creating concrete instructions based on the discussion, that the participants commit to following. The idea is to create the instructions as a compromise between the past experiences of the participants and what is expected of them in the policy. This means that changes are actually being made also on the side of the organization as well to facilitate rightful compliance activities. Having a trusted colleague as a dedicated resource to help employees both with technical information security issues as well as consult in case the employee doesn't know what to do helps in relieving complexity, overload and uncertainty in the workplace. (Ament & Haag 2016.)

Topic	Stressors/Description	Researchers
Work environment	**Complexity** (security requirements are time consuming, difficult to understand and ambiguous) **Overload** (security requirements cause extra workload) **Uncertainty** (there are constant changes and updates to security requirements)	Speier et al. 1997; Herath & Rao 2009; Hedström et al. 2011; Stahl et al. 2012; Guo 2013; D'Arcy et al. 2014; El-Den et al. 2014; Ament & Haag 2016; Albrecht 2016; Lee et al. 2016; Murtaugh 2017; Hoyle 2017
Personal environment	**Invasion of privacy** (the organization is monitoring and controlling employees' security behavior)	Lee et al. 2016; Ayyagari et al. 2011; Ament & Haag 2016
Social environment	**Conflict** (conflicting expectations on how to act, stigma) **News** (reactions to reports about security gaps & incidents, security warnings)	Herath & Rao 2009; Ament & Haag 2016; Anderson et al. 2016; Shackelford 2017
Ways to combat	Confidence in personal security skills Desired changes to the information security policy Better ways of communicating information security requirements Training	Karjalainen & Siponen 2011; Guo 2013; D'Arcy et al. 2014; El-Den et al. 2014; Ament & Haag 2016

Table 2 Summary of SRS environments and stressors from scientific literature

In a similar fashion as for technostress in chapter two, Table 2 summarizes the key findings from scientific literature on security-related stress. As both the literature on technostress and security-related stress and have now been reviewed, the first research question of what the two areas of stress have in common can now be answered. The following

part of the thesis will present the research design and empirical findings of the research in order to get clarity on the two latter research questions on why and how employees experience security-related stress and how organizations can improve their information security practices to prevent and reduce such stress from arising.

4 EMPIRICAL RESEARCH DESIGN

This chapter will introduce the chosen research approach and the methodological choices of this thesis, along with a description the data collection and analysis procedures used. This research will use the qualitative research approach and it will be conducted as a semi-structured theme interview. The design of the research is illustrated in the operationalization chart (Table 3).

4.1 Research approach and methodological choices

As the aim of this research is to go deeper into analyzing the subjective, personal experiences of individual employees than all previous SRS research which has been done quantitatively through questionnaires, the qualitative research method is the appropriate choice. Furthermore, out of the many different types of qualitative research – such as grounded theory, phenomenology and ethnography – narrative analysis will be used for the purposes of this thesis. According to Merriam (2014), narrative analysis uses stories of experiences told in first-person form as data. Narrative research is often used for instance in biographical research where interviewers ask the interviewees to tell their life stories (Flick 2009). The data collected through interviews for this study can be considered narrative, as the interviewee gives answers through stories, feelings and experiences related to the phenomenon that is being studied.

An interview can be described as a conversation between the interviewer and the interviewee, in which the interviewer initiates and leads the conversation to get insights on the interviewee's thoughts (Eskola & Suoranta 1998). For this research paper, data will be collected through individual face-to-face interactions in the form of theme interviews using the semi-structured interview method. In a theme interview, the interviewer divides the topic into different themes and makes sure all the same themes are covered with all the interviewees (Paavilainen-Mäntymäki 2017). Usually a theme interview does not include pre-drafted questions, but when mixed with a semi-structured interview method, the questions are made before-hand. According to Brinkmann (2013) face-to-face interviews give the richest data if analyzed properly. This is due to the fact that the face-to-face interview gives the interviewer additional insight from for example the non-verbal communication signals of the interviewee and the atmosphere of the discussion. For the purposes of this research paper, an individual interview will be the method of choice, as the topic of information security and stress can be sensitive and personal to the participants.

The operationalization chart (Table 3) below acts as a framework for planning the empirical research of this thesis. The table illustrates the purpose of the research and the path

from the research questions to the interview questions. As the interviews will be conducted as theme interviews, the appropriate themes are listed in the right-hand side column. It is also worth mentioning that since the first research question ("What do technostress and security-related stress have in common?") is addressed in the literature review in chapters two and three, it is not included in the operationalization table.

Purpose of the research: To find out how organizations can improve their information security practices to reduce security-related stress amongst employees			
Research Question	**Theoretical background**	**Sample questions**	**Themes**
Why and how do employees experience security-related stress?	"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" (Ament & Haag 2016)	Do you feel as though there are constant changes in the information security practices of your organization? How do you feel about your organization monitoring your information security behavior? What reactions do reports about information security incidents cause in you?	- Work environment - Personal environment - Social environment
How can organizations improve their information security practices to prevent/reduce security-related stress?	"The behavioral security research links numerous factors, including organizational sanctions, individual dispositions, security-related attitudes and beliefs, and workplace context, to name a few, to employees' security compliance decisions." (D'Arcy et al. 2014)	What could make you feel more confident about your information security skills? What would you wish to be changed in the information security policy to make it easier to understand or more encouraging?	- Preventing and reducing stress - ISP (Information Security Policy) compliance

Table 3 Operationalization chart

4.2 Data collection

The data for this research paper is collected by interviewing members of the staff of the University of Turku. As a large organization with many different job roles, the University of Turku has many different information security end-user profiles, which makes it ideal for getting a broad understanding of the negative effects of information security practices on different parts of an organization. The interviewees are chosen on the basis of their job roles, with the aim of getting as many different profiles as possible. When choosing who to interview, the number of interviewees was approximated by estimating how long it will take until the answers between the interviews start to repeat themselves. Twelve persons were approached, out of which nine answered affirmatively. The interviews were conducted within the time span of four weeks, and varied from thirty minutes to an hour in length. The final interviewees are listed in table 4. All interviews were recorded. As can be seen in the third column of table 4, while the job roles vary, there are comparatively more interviewees with an academic role (professor, lecturer or researcher) as the study aims to get as realistic of a sample of the employees in the environment of the University of Turku as possible, where most employees have an academic job role.

Interviewee	**Number of years in current position**	**Job role**	**Duration of interview (rounded to closest quarter of an hour)**
Interviewee 1	2	Planning officer for educational affairs	30 min
Interviewee 2	10	Executive secretary	1 hour
Interviewee 3	5	Professor	30 min
Interviewee 4	4	Departmental coordinator	30 min
Interviewee 5	5	Communications director	1 hour
Interviewee 6	5	Adjunct professor	30 min
Interviewee 7	4	University lecturer	45 min
Interviewee 8	5	Post-doctoral researcher	1 hour
Interviewee 9	6	University lecturer	45 min

Table 4 Interviewee profiles

The interview was constructed out of four themes, which are illustrated in table 5. The four themes were chosen on the basis of the two research questions, of which the first is

divided into three categories according to Ament & Haag's (2016) conceptualization of security-related stress.

Theme	Description
SRS and the work environment	The complexity, overload and uncertainty caused by organizational security practices and policies
SRS and the personal environment	How information security practices invade the privacy of employees
SRS and the social environment	Effect of conflicts and news on security-related stress in employees
Preventing and reducing SRS	Ways to make information security practices easier to understand and follow

Table 5 Description of interview themes

The interview questions (Appendix 1) were drafted in a semi-structured manner, using the survey questions of Ament & Haag's (2016) empirical study as a basis. The interview questions were open, as is typical for a semi-structured interview. The interview was structured to first find out the background of the interviewee's information security skills and knowledge as well as the interviewee's attitudes towards the information security practices and policies of his or her organization. The interview then continued with questions about security-related stress experienced by the interviewee in the different environments (work, personal and social) and finally concluded with the interviewee's thoughts on how information security practices and policies could be made less stressful. All in all, the interview consisted of twenty questions, which were asked in either Finnish or English, depending on the preferences of the interviewee.

4.3 Data analysis

In the context of research, data analysis aims to mine the most important findings related to the research question out of the research data (Saaranen-Kauppinen & Puusniekka 2006). There are numerous different approaches to qualitative data analysis, which all have the goal of studying the data in a systematic fashion. In this research paper, the primary data gathered from the interview was analyzed using the deductive content analysis method, which according to Tuomi & Sarajärvi (2009) consists of the reduction of data, the categorization of data and the abstraction of the results to fit the theoretical background of the phenomenon.

The first part of the deductive content analysis as defined by Tuomi & Sarajärvi (2009) is devoted to the reduction of data. In this study, the interview is first transcribed, checked and then read three times with different focuses. The first reading is to get a general idea about what the main ideas of the interview contain. The second reading is devoted to highlighting the most important findings of the interview, and the third to extract the main findings into a separate document. As the interview is conducted in either Finnish or English, the third part of the reduction process also includes translating the transcript into one common language. The second part of the analysis – the categorization of data – is made easier as the data is collected in the form of a theme interview. According to Saaranen-Kauppinen & Puusniekka (2006), thematization is a natural choice of analysis method for analyzing data gathered through theme interviews. In this method, the transcribed data is organized according to interview themes. The structure of the findings and discussion of this research paper follows the structure of the interview conducted. The final part of the deductive content analysis is the abstraction of data. This means looking at the data and comparing it with previous scientific theories (Saaranen-Kauppinen & Puusniekka 2006). As the research model is based on two previous studies by D'Arcy et al. (2014) and Lee et al. (2016) combined with Ament & Haag's (2016) own findings and technostress research, which are mirrored to the findings from the interviews.

4.4 Evaluation of trustworthiness

While the trustworthiness of quantitative research is often measured through the concepts of reliability and validity, these are not as such directly applicable to evaluating the trustworthiness of qualitative studies (Eriksson & Kovalainen 2008). According to Lincoln & Guba (1985), the trustworthiness of a qualitative study can be measured using four different criteria: credibility, transferability, dependability and confirmability. The trustworthiness of this research paper will be viewed through the lens of these four criteria.

The credibility of a qualitative interview study can be determined by critically assessing whether the conclusions drawn from the how trustworthy the subject of the interview and his or her opinions are. According to Merriam (2014), the qualitative research approach adds the risk of biases and other human weaknesses to the trustworthiness of the study, as the researcher as well as the subject of the interview play a large role in collecting and interpreting the data used for the research. According to Eriksson & Kovalainen (2008), credibility means that if another person were to read the text, they would come to the same conclusions. Transferability refers to the level of similarity between different studies and research on the same topic (Lincoln & Guba 1985). Due to the fairly new nature of the phenomenon of security-related stress, transferability is ensured because this research paper is built on all previous research available on the topic, and the

results are examined in parallel with the previous research. The whole outline of the interview, as well as the theory, is exclusively related to all existing research on the same topic. Dependability of a qualitative study means the extent to which the results of the study would be similar if the study were to be conducted in another context (Lincoln & Guba 1985). In the case of this research paper, dependability is ensured through the interview questions, have been drafted in a way that they can be asked at any organization where a security policy exists. However as the concept of stress is something that is experienced in a different way depending on each individual (Srivastava et al. 2015), and as organizations have different types of information security policies, there is no guarantee that the results of the study – if it were to be conducted in a different environment – would be exactly the same. Dependability can also be viewed through how transparent the research process is (Eriksson & Kovalainen 2008). Finally confirmability – which is the level of objectivity of the research – can be evaluated by assessing if any bias or underlying motivations affect the results of the study (Lincoln & Guba 1985). Any bias from the part of the researcher is mitigated in this research through attempting to analyze and evaluate the results of the research against the backdrop of previous research and the theoretical background used.

5 RESULTS AND DISCUSSION

This chapter will present the results of the empirical study and discuss their connection to previous scientific literature on the topic of security-related stress. The results are presented under the four themes introduced in chapter four – SRS and the work environment, SRS and the personal environment, SRS and the social environment, and preventing and reducing SRS.

5.1 SRS and the work environment

As identified in previous research (Ament & Haag 2016), the theme of security-related stress in the work environment consists of complexity, overload and uncertainty. From the interviews, it became apparent that complexity – which according to previous research arises from security requirements being too difficult to understand or comply with (D'Arcy et al. 2014) – was not something that bothered the interviewees, mainly because they didn't even know about the existing requirements. The information security policy was in fact one topic of the interviews that provided nearly unanimous reactions from the interview subjects. Most interviewees had not read the information security policy, but there were some instances where parts of the policy had been looked at to find some specific guidance on a certain topic. The fact that the information security policy was not even familiar to the interviewees is something that has not been considered in previous research on security-related stress. The general attitude towards the information security policy was quite dismissive. For example, one employee had browsed through the document to find out the university policy regarding the use of cloud storage services, but even in that case the interviewee chose to not follow the instructions clearly stated in the policy. Another employee had read the policy out of obligation due to being a member of the university's steering group on security, but couldn't recall in any way how it was structured or what it entailed. Even if an employee did remember having seen the information security policy at one point or another, they quickly went on to say they had no idea what is was like. Most of the interview subjects either didn't know if such a document existed or knew of its existence but had never felt the need to seek it out.

> *"Somehow it would be really nice if there was some kind of specific guidance somewhere. Might be that there is, I just haven't happened to find it"*

> *"I have no idea, well I think like I can't really even say if it exists and where you could find it – I can't answer to either of those questions"*

A very common opinion seemed to be that since the university is filled with so much information and so many documents, it was unreasonable to think that the employees would have time to go through all of them. Employees were more likely to go with their gut feeling when it came to security, or purposefully not pay attention to any information security rules because they didn't find them necessary, which is in line with the findings from Herath & Rao (2009). A good example of the phenomenon came from an interviewee who – as a side note – mentioned that she always left her computer unlocked with all systems running, but didn't even recognize that such behavior could somehow be harmful to information security. When asked whether or not there was any guidance on how to dispense students' grades for instance, one employee stated that the guidance probably does exist, but that he had no idea what the university's policy on that was and that it would require the employee to actively go read about it somewhere – which was too much to ask.

> *"I don't follow that stuff, or like where you can find what, the university is full of all kinds of documents that have nothing to do with everyday work"*

Employees seemed to therefore be experiencing information overload on a general level in their work environment, which in turn lessened their interest and capacity to handle information security related information. This issue of information overload in the organization was very apparent, and seemed to cause frustration within the employees no matter which position they held. One possible explanation for the negative attitude towards having to go through any additional information in their work could be in the nature of the work of an organization such as the university. As employees are usually teachers and experts in their specific field, and have to constantly read new content such as research or student essays, they may have even more information presented to them than would be the case for employees of other types of organizations. One employee, who represented the other side of the coin as her job role entailed communicating about various different topics to various different stakeholders, emphasized the importance of communicating things in the right tone to the right target group at the right time. She felt that a topic like information security could easily be made into something scary, and often ended up being dramatized to an excessive degree, which in turn took away from its credibility. On the other hand, she did recognize that there was a need to communicate about information security in general in the organization to raise awareness and make sure that the employees know which things to pay attention to.

In terms of information security in specific causing work overload in employees, some good examples– which correspond to the findings from previous research on the topic – were given by the research subjects. An employee described a common nuisance that she

faced in her work, where due to security restraints she did not have access to certain information in a system she often used, and therefore had to always ask for the information from someone who did have access. The interviewee found the situation frustrating and inefficient, because in any case the information was always provided to her, but still she was not allowed access to the system. Such addition to workload from access restrictions was also identified in the research by Lee et al. (2016) and Ament & Haag (2016). Another example of work overload came from an interviewee who had started working on a research project which had already been granted funding, but then got cancelled at a very late stage due to one of the lawyers from the project contractor's side deciding that the project couldn't be continued as they weren't sure their data was completely safe. The researcher had ended up going through policy documents to try to find answers to questions, but hadn't found any information that would've suited his purposes. Similar situations, where security-related stress comes from having to invest significant amounts of time in going through and trying to understand security requirements, are described in research by D'Arcy et al. (2014). The situation described by the interviewee could be characterized as the very worst-case scenario for such situations, as the time invested in trying to understand the security materials ended up being time wasted as no answers were found and the project ended up not being rolled out. The third instance where information security added to workload, ultimately causing a security conflict was one where, for research purposes, a researcher had to play a certain game, which the university end point protection didn't allow access to. As the interviewee was unable to turn off the protection because it was managed centrally in the organization, he had to take his home computer, turn off the virus protection and play the already questionable game without any computer protection. Such non-malicious violation of the security practices has also been identified in the research by Guo (2013).

Despite the examples of information security overload identified in the interviews, most employees felt that information security was hardly anything they ever thought about, meaning that it was more likely for them to ignore anything that would add to their workload rather than take the time to find out how to act. There were also instances described in the interviews that matched those of previous research – such as an employee having to always dispose of certain sensitive materials after reading them – which were seen as such an instilled part of the employees' work routines that the interviewees didn't find them to be a burden. In that sense D'Arcy et al.'s (2014) finding of overload from information security leading to employees having to take time away from their actual work did not apply, since employees felt that information security was part of their actual work. A possible reason for hardly thinking about information security or even ignoring it altogether could be a lack of realization of the consequences of security breaches. Employees seemed to be working in their own silos and it could be sensed that because they

knew that someone else was in charge of information security in the organization, employees also felt that whatever breaches might happen would not be traced back to them because it would in the end be the fault of the information security officer.

The third SRS stressor in the work environment – uncertainty – has in previous research (D'Arcy et al. 2014; Ament & Haag. 2016) been found to arise from the constantly changing security requirements that are required due to the fast pace of technological change. From the interviews it became apparent that there was already so much uncertainty regarding the existing security requirements, that the interviewees simply didn't have the interest or the capacity to keep up with what and how the information requirements were changing. On the other hand, any such changes weren't even being communicated, at least in a way that would have caught the interviewees' attention. A common opinion was that the interviewees had never received any communication about either the information security policy or any changes related to it. The findings on security-related uncertainty are therefore not in line with previous research on security-related stress. For instance with the upcoming GDPR, most interviewees had never heard about the university's stance on the new regulation. Those who had heard of some initiatives from the university to react to the changes brought along by the GDPR were persons who were somehow involved in defining how the reform will affect the university. The interviewees who felt as though they had never received any communication about the information security policy or changes to it, were also quick to disclaim the statement by bringing to light the issue of the university having so much information generated and communicated on a daily basis that it was impossible for an employee to process all of the information. This finding binds together the two stressors of uncertainty and overload, because the same constant stream of information is mentioned as one of the causes of techno-overload from technostress research as defined by Ragu-Nathan et al (2008).

> *"Well I have to say now that it feels as though these changes are just happening somewhere else and like I'm not getting any information on them and I don't know how to somehow start to educate myself or follow what's changing, so no it doesn't feel like it's something that affects me"*

In fact, while the stressor of uncertainty is mainly defined in both SRS- and technostress research as something that is caused by change (D'Arcy et al. 2014; Ament & Haag 2016), the general feeling from the interviews was that more uncertainty from information security was caused due to a lack of knowledge, guidance and control. In all interviews, at some point each of the interview subjects in one way or another stated that they are aware that they should probably be more aware when it comes to securing their data. In the same way, interview subjects seemed quite embarrassed about their lack of

knowledge which points to the fact that they felt as though they felt that they should have been aware of the answers.

> *"And then it made me feel a little like I should probably know something about this when you asked me [for an interview] or that should I somehow know way more about this really"*

When asked how confident the employees felt about their own information security skills, there was a lot of uncertainty to be sensed. None of the interviewees felt that they were completely confident when it came to own information security skills, however most subjects stated that they weren't especially worried either. An interesting finding regarding employees' information security practices was that all interview subjects seemed to feel to some extent that they were not responsible for information security, but rather that information security was the responsibility of their employer.

> *"…and I haven't really thought about whether or not I could send this or that [regarding salary information] and then I feel that it's the university's responsibility that if someone breaks into the system that it's not like my then… or that my head won't be on the chopping block"*

Another common theme in the answers was that since they had never had to face any major information security issues, employees felt that their current knowledge – which all subjects identified as very limited – was sufficient for the time being. The effect of having been victim to security breaches earlier on current information security behavior is something that has not been touched before in SRS research. It was very interesting to see the internal struggle experienced by interviewees on this topic, as there was a certain inconsistency and illogical nature in the answers. The phenomenon seemed ubiquitous: at the same time not being too worried about information security, but feeling insecure about own information security skills and feeling as though one should be more competent when it came to information security.

> *"I still kind of feel that I'm quite bad in some sense, like I don't think about information security stuff too much somehow that like maybe I'm able to avoid the biggest pitfalls but… then I'm pretty satisfied I haven't noticed that I should care more"*

Nearly all of the interview subjects stated that they had no idea what to do in case an information security breach were to happen. There was a clear conflict between how the employees felt that they should be more aware and more competent in their information

security practices, but at the same time finding themselves not caring enough to do something about it – also identified in the research by Lee et al. (2016). Interviewees also mentioned that they were worried about the future of information security as they realized that in it's current state it is not really taken seriously in the workplace. This has not been taken into consideration in previous research in security-related stress.

> *"... I don't take [information security] for granted though, somehow I mean that it's like something that comes as services develop and digitalization develops, then through that development the role of information security will also in my opinion grow"*

Overall, the empirical findings of SRS in the work environment from this study found factors that were in line with previous research, factors that contradicted previous research and entirely new areas of stress that could be further studied. Contradictory to previous research (D'Arcy et al. 2014), complexity did not appear as a stressor in this study, mostly due to the fact that employees had not read any information security materials to begin with, let alone find them complex. Similarly, uncertainty as a stressor in the work environment was not perceived as in previous research as arising from constant change (D'Arcy et al. 2014; Ament & Haag 2016), but rather from not having enough know-how or knowledge on security issues and ways of combatting such issues. A finding that was in line with previous SRS literature (Herath & Rao 2009; Guo 2013) was that employees were engaging in non-malicious security breaches. However, in previous research this has been linked to the stressor of complexity (D'Arcy et al. 2014), while in the realms of this study, it seemed that the cause of non-malicious incompliance was in fact overload. Previous findings on information security overload (Lee et al. 2016; Ament & Haag 2016) were to some extent supported by the findings of this study, for instance in terms of having to spend significant amounts of time in trying to understand what is expected or being faced with access restrictions which caused extra workload to employees. However, this research also brought to light a previously neglected area possibly affecting information security compliance, which was the overall information overload affecting employees' capacity to process security-related information.

5.2 SRS and the personal environment

In previous research, SRS in the personal environment has been found to be caused by a stressor dubbed by Ament & Haag (2016) "invasion of privacy". Research has shown that SRS could stem from employees feeling as though their privacy is being invaded when their employer is monitoring their information security behavior (Lee et al. 2016). In the

empirical findings of this study, employees did not know whether their employer was monitoring their information security behavior, however all of the interviewees felt that it was a realistic possibility. This – referring to the incomplete knowledge of whether or not such monitoring is happening – is in fact exactly what has been defined as the core reason for SRS in the personal environment by Ament & Haag (2016). One employee, who used to run another business alongside his university position, described a situation where the other business' e-mail address was linked to his university e-mail in a way that allowed for all the incoming e-mail to come to the same mailbox. The IT department had noticed that there was unusual incoming traffic to his e-mail, and contacted the employee to ask what was going on.

> *"They came from the helpdesk all serious asking what's up with you having some, you have this e-mail profile and I was like okay this is what it is, well in my understanding it wasn't even a problem, I don't know, well maybe it was like an indication of them observing…"*

The employee remembered at the time wondering to what extent the organization was monitoring him, but found it hard to believe that they would go to the extent of looking at the websites he visits for instance. He strongly felt that the right thing to do would be to inform people of such activities and be as transparent as possible if monitoring was going on. On the other hand, another employee felt very nonchalant about the idea of the organization monitoring her, as she believed that none of the information she had on her computer or her phone – both of which she also used as her primary personal devices, which meant that all her personal information was also stored in them – would be of interest to anybody. From the interviews in general, it seemed that the more concerned an employee was about the organization monitoring them, the more security conscious they also were about other issues.

An interesting finding was that the range of different opinions when it came to the question of whether or not it would violate an employee's privacy if the organization would be monitoring the employee, was very wide. While some felt that the act of monitoring was a complete violation of their privacy and fully unacceptable, others either didn't care about it or even found monitoring necessary. One interviewee was of the opinion that as long as the organization was acting under the Finnish law, it would even make the employee feel more secure if the organization was monitoring its employees' behavior, because it would mean that all suspicious behavior would then be investigated. Another employee very strongly stated that it would be an invasion of his privacy to monitor his behavior on the Internet, but also found it hard to believe the organization was doing such activities. A key finding from the side of SRS and the personal environment was that none of the employees really knew whether or not such monitoring was happening

from the side of their employer, which also caused them to have to guess. Not knowing exactly what was being monitored made interviewees feel uneasy and confused. This is in line with Ament & Haag's (2016) finding that the stress that is caused by invasion of privacy comes specifically from not knowing whether or not the employer is engaging in monitoring activities.

> *"Well actually I don't', umm this is also one of those things that I don't really know exactly but I would assume that yeah some kind of, some kind of monitoring… or I mean I don't think that anyone is reading… or in a sense yes but I don't really know what it means in practice"*

One of the interviewees shared an experience which had made her cautious of the IT department and everything they had access to. The employee was faced with a fundamental technical issue with her computer, so she took it to the helpdesk to be fixed. The IT experts had asked her some technical questions which she hadn't fully understood, leading her to accidentally give consent to the computer being fully emptied without backing up the files.

> *"It was some word IT uses which I missed that I apparently had then said okay to, and [my computer] was completely emptied, I lost for instance two years' worth of photos. It was an absolutely horrible situation… So really after being through something like this I've become pretty careful in the sense of what [the IT guys] can actually get to and what it could mean in the worst-case scenario"*

The employee emphasized the outrage that she had felt from the fact that she had been expected to understand the technical terms used by the information technology professionals and having been put into the position of having to make a decision when she clearly wasn't in the position to make such a decision. The reason why this is so interesting, is because it ties into the theory by Ament & Haag (2016), that has so far not been supported by quantitative research, that SRS can also result from a stressor called Degree of Freedom. Degree of Freedom as a stressor in Ament & Haag's research could derive from an employee having been given the freedom and responsibility to make decisions when they don't feel equipped or confident to make those decisions. The third security-related stressor in the personal environment, job insecurity, which was also theorized but not proven by Ament & Haag (2016) did not manifest itself in this study either. Job insecurity in the context of SRS was characterized in theory as the fear of losing one's job due to not being competent in information security matters.

All in all, the presence of SRS in the personal environment as defined by Ament & Haag (2016) as invasion of privacy was supported by this study. However, the findings also showed that for some employees, the monitoring seemed to have a positive effect on their level of comfort regarding the status of information security in their workplace. This has not been found to be the case in previous SRS research. The findings supporting "degree of freedom" as theorized in previous research were a new contribution to the field of SRS, as earlier studies have not been able to confirm such stress appearing in the personal environment.

5.3 SRS and the social environment

Security-related stress in the social environment has been identified in previous research to result from both conflicting expectations regarding security behavior and from disconcerting news about security breaches (Ament & Haag 2016). When asked to identify situations wherein the employee had been asked by a superior or a colleague act in a certain way that the employee knew was contradictory to the information security policy of the organization, the interviewees were able to recognize such situations from their professional life. One interviewee described a situation that happened on a recurring basis, where she was put into a position to have to receive sensitive information about students in the form of Excels via unencrypted e-mail. The interviewee herself felt that this information should have been secured somehow or rather been stored in a secure system, but because her colleagues at the other university where the material was sent from were not concerned about any security issues, there was little to be done in the way of changing their behavior. This is an example of conflicting expectations, which in Ament & Haag's (2016) research was described as situations where employees are faced with a conflict as they are in a way forced to act in a way that disagrees with their own information security knowledge or standards. Another employee recognized a similar issue, where sensitive information was stored in an Excel and could easily get into the wrong hands.

> *"I've sent information in these Excels, imagine how vulnerable they must be since they're not behind any system… In that way you really could, I'm sure in many organizations talk about these "Excels" so to say, you can find those here too"*

According to the interviewee, the creation of so-called "shadow registries" was also something that occurred on an ongoing basis. These registries were employees' own collections of student, alumni and company information, which were created by employees to avoid having to always ask for needed information from someone when needed. The

reason why the interviewee felt this was problematic, was that it led to not knowing how the information was being used and by whom, as opposed to the correct procedure of storing the information into a secure system which would always record stamps as evidence of when and by whom information was retrieved. The creation of these shadow registries was also a problem from the side of data quality, because it meant that certain employees had different versions of for instance contact information for the alumni because the information was only updated in the system. This lead to misunderstandings, not being able to reach the right focus groups and in the worst cases situations where wrong things were communicated to wrong people. One interviewee described such a case where an e-mail had gone to a much larger distribution list than it was supposed to, and remembered the situation as very stressful. Luckily the information in the e-mail had not been of a sensitive nature, but it was however irrelevant to a lot of recipients who then opted to respond by demanding to have their contact details removed from the university's registry.

One employee had been in a situation where she had asked for some information about certain members of a certain user group, and was instead given the entire user registry with information about all the members. The reason behind being given all this information was that the employee's colleagues said that they didn't have the time or the resources to start parsing through the long lists for individual pieces of information, and that she would have to go through the materials herself. As the interviewee characterized herself as very safety-conscious, she remembered feeling uneasy about the careless way in which the information was handled and distributed in the organization, because she felt that she shouldn't have gotten access to this information.

> *"But it was kind of one of these situations where I thought that okay this is how things are done, because I felt that I was in a way a complete outsider for even asking for this, of course I'm part of the organization but not directly in the user group [that would see this information], and then they decided to go with this solution"*

As Ament & Haag's (2016) view of SRS arising from conflict has been described through other people's expectations conflicting with the information security policy, the interviews also revealed situations where employees knew they were – for their own reasons – acting against the information security policy, simply because it was much more practical to do so. This is in line with Herath & Rao's (2009) finding that sometimes the information security policy is neglected due to convenience. A common example was the use of the cloud-sharing environment Dropbox instead of the university's own cloud environment even though employees knew that the use of Dropbox was discouraged in the university's information security policy. One employee stated that she and her colleagues

had decided to go against the university's policy on Dropbox "this one time" because they felt that the form they were sharing wasn't that critical. Another employee had decided to take Dropbox into everyday use because it simply made his work much easier.

> *"University policy says that we shouldn't use Dropbox, but I do. The reason for that is that our internal option which is called Seafile doesn't offer the options which I need – I can't share editing rights with externals and I co-author all the time with people from all around the world"*

In fact, the situation described by the employee could also be seen as a conflict arising as a result of overload, which is a stressor occurring in the work environment first introduced by D'Arcy et al. (2014). Acting according to the university's information security guidelines would have added to the workload of the employee, because it would've meant he would have always had to receive different versions of the master document via email, then update the master document and share it with the other parties.

Another form of conflict situation could according to previous research (Ament & Haag 2016) be stigma from fellow employees from being too compliant when it came to information security. From the interviews, the employees were unable to identify instances where they had seen colleagues have stigma against employees who took information security seriously, but rather that if someone was very security aware, people felt like they should be acting in the same way. There were, however a few mentions of the interviewees themselves having some stigma against very security-oriented employees. For instance, one interviewee identified a frustrating situation, where her department had to collaborate with the IT-department on a project, but whenever asking the IT professionals to share any information with them, the answer was always no. This lead to the interviewee feeling as though they were strictly following security guidelines out of spite. Another interviewee shared an experience from when he first started working at the university and was placed in a team where information security was taken very seriously. He couldn't understand the point behind taking security so seriously, because he felt that the information they were producing wasn't something that needed to be hidden.

> *"...but I was always wondering, well why? Or like my point was that okay if we have some information that someone would want, well I do research, I want everyone to get the information I produce!"*

News and reports about security gaps at work or in the technologies the interviewees used were of interest to the employees, but didn't for the most part seem to bother anyone too much. However, many of the interviewees mentioned feeling that they were being naïve and too trusting with the systems they were using. This is in line with Anderson et

al.'s (2016) findings of there being an inconsistency between how worried users are about information security issues and how much (or actually little) effort users are putting into preventing those issues.

> *"I don't really care that much, I should. I mean privacy and security – and for me security is mainly about privacy – I have some documents on my computer which shouldn't fall into generic hands because I do some EU projects and some of them are… I mean I've signed a bunch of NDAs and stuff…"*

In the same way, Anderson et al.'s (2016) findings about employees growing too accustomed to seeing security warnings pop up on their screens for them to have any effect was also in line with the interview answers. Either employees couldn't recall how they reacted to their antivirus software notifications or then they usually chose to ignore the notifications.

> *"Just today I was thinking that maybe before somehow I've worried about [information security] more because there's been more talk about all the kinds of risks that exist, and perhaps back then I thought about whether I would actually know how to act in all those situations. But maybe nowadays I think that somehow I'm pretty confident. However in practice it doesn't mean… or that maybe it's just that I'm trusting that the systems work"*

Some examples of reports about information security incidents that were mentioned by the interviewees included friends' Facebook accounts being hacked into, backups failing and lists of passwords into systems being leaked to a wide audience. One interviewee stated that whenever she read an article about a security incident or a gap in a system she used herself, she felt as though she needed to go check her settings. This is in line with Ament & Haag's (2016) finding that people who experience stress from security news are more likely to be more security-conscious. Another interviewee described an opposite reaction to security news, as the employee said that there had been so many rumors about Whatsapp being hacked into, but they seemed to never be true so he wasn't bothered by the news and continued using the application for sharing work-related things without knowing if it's allowed.

When it came to reactions to larger security incidents, for instance the two ransomware attacks of the summer of 2017, the most common opinion was that the attacks felt very distant and unlikely to happen at the workplace of the interviewees. Most of the interviewees remembered hearing about the security breaches of the summer and thinking

about it for a second but not feeling worried. One interviewee stated that while he felt a little worried, it just in fact reinforced his habit of backing up his files on the regular as not to lose anything if something like this were to happen. This is another good example of the security-reinforcing side-effects of security-related stress from news (Ament & Haag 2016). On one extreme, an employee felt that the university didn't have any money or sensitive information that would be useful for anyone hacking into their systems, and that on the other hand even if something were to happen that would destroy files in the organization, it wouldn't be too much of a loss because surely the university had backups for most of the computers. Another, more security concerned employee felt that there was a very concrete risk for ransomware or other information security incidents happening at the university and causing damage.

> *"I remember thinking that what if that had happened to us, I would have no clue how to act."*

SRS in the personal environment as a theme in the interviews also exposed many of the employees trusting the university to take care of information security for them. One interviewee talked about feeling very contradictory, because he relied on the university's systems with what he described as naïve trust, all the while knowing that incidents like WannaCry and Petya do happen all the time. Therefore the research by Ament & Haag (2016) which found that news of big security incidents that are broadcasted largely in the media cause stress is valid, however in order for such stress to lead to positive outcomes such as more compliant behavior as theorized by the researchers, the incidents would have to be much more relevant to the employee, either by being happening to someone they know or by affecting a system they use frequently.

On the whole, SRS in the social environment was most in line with previous research in the field (Ament & Haag 2016; Herath & Rao 2009; D'Arcy et al. 2014; Anderson et al. 2016) from the three different environments of the conceptual model of SRS. Both stress from conflicting expectations and stress from security-related news were found to appear in the interviews, however at most moderately. A new finding that at the same time agreed with previous research regarding collective stigma against employees who were considered too security compliant, showed that while some interviewees themselves admitted to judging their very security-conscious colleagues, employees mostly in fact appreciated anyone who had any extra knowledge about information security in the organization. While the stressor of news – especially in the light of recent media coverage of big ransomware attacks – had made the interviewees worry to some extent, it was not something that could be considered as a major cause of stress in employees, as they found it highly unlikely that they would ever be faced with any information security breaches.

5.4 Preventing and reducing SRS

Prior research on ways of preventing and reducing SRS has considered increasing confidence in security skills, changes to the information security policy, improvements in communication regarding information security and finally training as best practices (Karjalainen & Siponen 2011; Guo 2013; D'Arcy et al. 2014; El-Den et al. 2014; Ament & Haag 2016). In terms of suggesting ways to feel more confident about their information security skills, nearly all interviewees mentioned that they wanted to get clarity on information security guidance and better communication on what was expected of them. A common view was that there was very little or no communication about information security at the university. When asked how information security could be communicated most efficiently, the interviewees were fast to mention the modes of communication that did not work – from news on the intranet and generic alerts about obvious phishing e-mails, to posters on the walls and mentions in the weekly e-mail.

> *"I really believe that all employees somehow adopt the culture of the place they work at, so if it [information security] isn't something that's talked about then maybe people don't understand the significance it could have"*

D'Arcy et al. (2014) suggest making the information security policy as user-friendly as possible, however in the case of the target organization, changing the outlook of the information security policy would not do much since most people have not read it. In fact, most of the feedback regarding the structure and language of the policy was surprisingly positive. One of the interviewees who had read the information security policy mentioned that even though she still found the current policy quite distancing and hard to get a hang of, she felt that the IT department had actually improved their output and text generation when it came to the policy. Another employee said that the information security policy was quite clear in how it was structured, and a third said that he didn't have trouble understanding the policy but that it was written in a very general way that didn't help him in his specific situation. In this sense the biggest issue with the information security policy seemed to be that the content had not been brought to the knowledge of the employees. One employee hoped for a list of the most common questions and situations to be presented in the information security policy, because he suspected that his questions about the GDPR for instance would also be on the minds of his colleagues. In their research, El-Den et al. (2014) suggested communicating the information security policy to employees through posters and leaflets with the help of visual aids. This idea was not supported in the interviews as an effective form of communication, as interviewees felt that posters and other such material always went unnoticed by the employees.

None of the interviewees had ever attended an information security training, and the common perception was that such training wasn't ever even organized. When asked if the employees would attend a training on information security, the answers were mostly positive albeit with some conditions. The employees who felt they would get something out of the training emphasized that the session would need to be very relevant and concrete, while bringing some actual value, for instance by being designed for specific user groups or on a specific topic such as the GDPR. This is in line with the study by Hedström et al. (2011), where value-based information security management is found to help in getting the message of the information security practices through. Even employees themselves stated that it would be easier to understand the need to comply with the university's information security practices if it was in line with their primary educational values. Similarly, some interviewees stated that they most probably wouldn't attend the training, either because they had so much going on that they would prioritize something over the training or find it useless because they wouldn't be able to remember the information anymore when it was actually needed. One interviewee said that so far the communication about security had been so generic and obvious that he felt as though a training would most probably be a waste of time for him. These findings were strongly in line with Lee et al.'s (2016) idea that employees who perceive information security breaches as a true threat are more likely to comply and want to educate themselves on how to better secure their information.

> *"In a sense it is a very interesting field, but if the content is on the level of like "don't give your passwords to anyone", then I wouldn't go ... but this would be a very relevant topic and like some good performer who would be able to present what all this means and what the future scenarios are from the point of view of our practical everyday working life, I would be interested"*

Regarding the content of the security trainings and communication, there were a lot of suggestions as to what the employees wanted to know. Concrete examples of actual security threats along with ways to both prevent them from happening along with clear rules on how to act if something were to happen were things that the interviewees were interested in hearing. This is in line with the suggestions of Karjalainen & Siponen (2011) as to what constitutes a good information security training. One interviewee suggested that the best way of getting the information to sink in would be if every time that some large security scandal happens, someone would send an information blast explaining what happened, how the university is protecting itself from similar things happening here and what an employee can do to prevent such things from happening. Communicating about the incident when it is relevant will leave a mark in the employee's mind all the while giving

a concrete context to the message. One interviewee hoped for someone to tell him why it was necessary in the first hand for him to be concerned about information security, since nothing had ever happened to him that would have made him feel as though he wasn't secure.

One employee mentioned that they had a concept called "Teacher's corner", where teachers and researchers gathered to discuss and brainstorm on different topics and themes. The employee felt that it could be a good idea to integrate information security training into the concept, because it would be a different, more engaging form of training where employees could learn through discussing amongst themselves. Such a concept would also be supported by the ideal structure of an information security training suggested in the research by Karjalainen & Siponen (2011), where learning would happen through the four phases of involving concrete experiences, engaging reflective observation, supporting formation of abstract concepts and generalization, and enabling active experimentation.

The findings from this empirical study regarding ways of combatting and reducing security-related stress were strongly in line with previous research on the topic (Karjalainen & Siponen 2011; Guo 2013; D'Arcy et al. 2014; El-Den et al. 2014; Ament & Haag 2016). The key finding in terms of what the employees themselves believed would work to increase their information security knowledge and skills was tailored and relevant communication. When it came to trainings as a way of reducing stress from information security issues, employees felt that they would be open to the concept of trainings, but that in order for there to be any benefit from attending, the trainings would have to be brought to the level of the employee, his or her everyday work and only be centered around realistic scenarios and threats.

6 CONCLUSIONS

The aim of this thesis was to provide insight on the question of how organizations could improve their information security requirements in order to reduce security-related stress in employees. The three research questions around which the thesis was built were

1. What do technostress and security-related stress have in common?
2. Why and how do employees experience security-related stress?
3. How can organizations improve their information security practices to prevent/reduce security-related stress?

The first question was addressed through reviewing previous scientific literature both on technostress and on security-related stress. One significant difference between the two concepts found was that while technostress is examined mostly through stressors –commonly divided into techno-overload, techno-invasion, techno-complexity, techno-insecurity and techno-uncertainty – and their effect on environments, security-related stress was examined through environments from the start. The three environments – work-, personal-, and social environment – did however include stressors that were present in technostress as well. Similar stressors in both fields included overload, complexity, uncertainty and invasion. The stressor of insecurity, which was identified in technostress literature was not its own stressor in security-related stress. This was interesting to find, because form the interviews, it felt as though all the interviewees were very insecure about their information security skills. Entirely distinct stressors identified in SRS research but not in technostress research were stress from news and stress from conflict. The similarities and differences between stressors from the two fields of research are presented in table 6.

Distinct technostress stressors	Stressors in both fields	Distinct SRS stressors
Insecurity	Overload Complexity Uncertainty Invasion	News Conflict

Table 6 Similarities and differences between technostress research and SRS research

The second research question aimed at finding out how and why employees experience security-related stress. As such, it seemed that many of the causes and consequences of security-related stress were a reality in the organization, however the employees did not

characterize or identify the situations in themselves as stressful. Based on the interviews, SRS appeared mostly in the personal environment and the social environment, whereas the security-related stressors of the work environment seemed to have less of an effect on employees. While some examples of complexity and overload were given by the employees, they were not considered to be major issues, as the information security policy and requirements in general seemed to be very distant and unfamiliar concepts to the interviewees. The only stressor that did seem to cause harm in the work environment was uncertainty. Uncertainty was mainly caused by the lack of knowledge, guidance and control regarding information security in the work community, emphasized by the fact that there was very little or no communication about information security in the organization. Another issue causing uncertainty among employees was worry about future information security, as employees identified their current skills in information security as poor. The stressor of invasion of privacy in the personal environment was also a cause for concern among the interviewees. There was a lot of uncertainty about the level at which the organization was monitoring the employees' security behavior. While not all interviewees felt that it would be an invasion of their privacy if their organization was monitoring them, it was clear that the monitoring should be transparently communicated. The general finding regarding news as a stressor was that while news about security breaches worried the interviewees, they felt that it was unlikely for similar security breaches to happen in their organization. Another finding was that employees seemed to feel as though they should have been more worried, but that they were naively trusting the organization and it's systems to be secure. Conflict regarding security behavior was present in the organization, both in terms of willingly acting against known requirements and in terms of being asked to act against the information security policy by a colleague or a boss.

All in all, it was surprising to see the extent to which SRS did exist even in an organization where employees did not seem especially security-conscious. A possible explanation to this finding, which was reflected in the interview answers, is that due to the extensive technological leaps that are being made in the field of information systems – which go beyond the understanding of employees – we are not only storing more and more information about ourselves and our work in a digital format but at the same time in fact not understanding how the information is stored, what the technologies mean, and what the risks are. Parallel to this phenomenon is the fact that as technology becomes more sophisticated, so do the security breaches. Adding to this the constant media coverage of security incidents, employees and individuals are left with the conflicting notion of having to – and even wanting to – trust systems they do not understand all the while understanding that the information security-related risks exist.

The third and final research question was also addressed through the interviews. The key finding about preventing and combating security-related stress was that while employees wanted to learn and be more informed in information security issues, they found

themselves falling short and losing interest due to bad communication. As suggested by literature, the idea of security trainings was supported in the interviews with the condition that the content would be relevant, understandable and concrete, explaining actual threats. Persons with more administrative roles in the organization seemed more concerned about information security than lecturers and researchers.

The biggest theoretical contribution of this thesis is that it provides new insight describing the appearance of the phenomenon of SRS in an organization, as this is the first qualitative study to have been conducted on the topic. As the interviewees were encouraged to describe situations from their everyday life, the findings also provide SRS research new real-life examples of the stressors– which have so far only been hypothesized by researchers. The finding that most of the stressors of overload, complexity and uncertainty in the work environment are not considered as true causes of stress by employees – at least in the way they are currently defined in the field – is a valuable theoretical contribution, as it could either point to the idea that different stressors of SRS appear in different organizational settings, or to the fact that by interviewing employees instead of studying the phenomenon quantitatively through questionnaires, a broader snapshot of the phenomenon from the point of view of single employees is revealed.

The practical implications of the findings in this thesis are useful for information security professionals as well as people in charge of the wellbeing of their organization. As based on the empirical findings there's a lack of communication between information security professionals and employees, this research can act as a glimpse into the thoughts of the end users, which in turn helps better understand ways to communicate and train employees and in turn improve the state of information security in the organization. Stepping into the shoes of an employee and looking at how information security is perceived through their eyes can help practitioners to better tailor their message in a way that is meaningful to the employee.

The limitations of this research study include the fact that the research concentrated on the employees of one specific organization in one specific country, which means that the phenomenon could be perceived differently in other settings. Another possible limitation is that while the researcher felt that a saturation point was reached with the number of interviews in this study, stress as a concept is very subjective, meaning that the specific situations and feelings described by the interviewees in this study could be very different for a different set of interviewees.

Future research should continue to examine the phenomenon qualitatively to gain a broader understanding of different views and further validate the findings from this research. The empirical findings of this research paper have first and foremost brought into light the negligent attitude and uninformed state of employees regarding information security. While the ignorance and incompliance of information security practices in organizations has been widely studied in the past, future research could address the stress that

is caused by the non-existent knowledge of information security among employees. Stress from uncertainty – which so far in SRS research has meant uncertainty from constantly changing requirements – could therefore be studied as in fact being caused by overall uncertainty about how to act, what is expected and what information security means. Another aspect of security-related stress that is closely tied to the uninformed and nonchalant attitude of employees towards information security is that of the effects of previous experiences with information security incidents affecting current compliance behavior. As many interviewees often justified their lack of cautiousness to never having experienced any issues and therefore not seeing any need to change their behavior, it would be interesting to study the effects and possible remedies of the phenomenon. Regarding SRS in the personal environment, which stems from employers monitoring employees' information security behavior, further research is needed to understand the effect of the setting in which the employees are working. The setting in this study was a Finnish university, where most employees relied on the Finnish law preventing their employer from tracking their behavior in a way that would harm the employee. The findings could be completely different for instance in a different country where the trust in authorities and lawmakers is not as strong.

7 REFERENCES

Ahmad, U. – Amin, S. – Ismail, W. (2012) The Relationship Between Technostress Creators and Organisational Commitment Among Academic Librarians, *Procedia: Social and Behavioral Sciences,* Vol 40, 182-186.

Albrecht, J. (2016) How the GDPR will Change the World. *European Data Protection Law Review (EDPL),* Vol 2 (3), 287-289.

Ament, C. – Haag, S. (2016) How Information Security Requirements Stress Employees. *Completed Research Paper presented at the 37th International Conference on Information Systems*, Dublin, Ireland, 1-17.

Anderson, B – Vance, A – Kirwan, C- Eargle, D. – Jenkins, J. (2016) How Users Perceive and Respond to Security Messages: A NeuroIS Research Agenda and Empirical Study. *European Journal of Information Systems,* Vol 25 (4), 364-390.

Angermeier, I. – Boss, S. – Boss, R. – Kirsch, L. – Shingler, R. (2009) If Someone is Watching, I'll do what I'm Asked: Mandatoriness, Control, and Information Security. *European Journal of Information Systems*, Vol 18 (2), 151-164.

Aurigemma, S. (2013) A Composite Framework for Behavioral Compliance with Information Security Policies. *Journal of Organizational and End User Computing,* Vol 25 (3), 32.

Ayyagari et al. (2011) Technostress: Technological Antecedents and Implications. *MIS Quarterly,* Vol 35 (4), 831-858.

BBC (2016) French Workers get 'Right to Disconnect' from E-mail Out of Hours. <http://www.bbc.com/news/world-europe-38479439>, retrieved 29.3.2017.

Blili, S. – Raymond, L. – Rivard, S. (1998) Impact of Task Uncertainty, End-Iser Involvement, and Competence on the Success of End-User Computing. *Information & management,* Vol 33, 137-153.

Booker, E. – Rebman, C. – Kitchens, F. (2014) A Model for Testing Technostress in the Online Education Environment: an Exploratory Study. *Issues in Information Systems,* Vol. 15 (11), 214-222.

Brinkmann, S. (2013) *Qualitative interviewing*. Oxford University Press, Oxford.

Brod, C. (1982) Managing Technostress: Optimizing the Use of Computer Technology. *Personnel Journal,* Vol 61 (10), 753-757.

Brooks, S. – Califf, C. (2017) Social Media-induced Technostress: Its Impact on the Job Performance of IT Professionals and the Moderating Role of Job Characteristics. *Computer Networks,* Vol 114, 143-153.

Caro, D. – Sethi, A. (1986) Technology Strategy: The Role of Strategic Planning and Monitoring Systems. *Human Systems Management*, Vol 6, 121-129.

Cate, F. – Kuner, C. – Svantesson, D-. – Lynskey, O. – Millard, C. (2017) The Rise of Cybersecurity and Its Impact on Data Protection. *International Data Privacy Law,* Vol 7 (2), 73-75.

Chakhovich, T. (2017) Tutkimusprosessi ja Kvalitatiiviset Tutkimusmenetelmät, luennot ja kirjallisuus. *YSM lectures, spring 2017.* Turku School of Economics.

Chandra, S. – Srivastava, S. – Shirish, A. (2015) Do Technostress Creators Influence Employee Innovation? *PACIS 2015 Proceedings*, Vol 93, 1-9.

Clark, K. – Kalin, S. (1996) Technostressed Out? How to Cope in the Digital Age. *Library Journal,* Vol 121 (13), 30-32.

Cleary, T. (2017) Petya/NotPetya Ransomware Attack: 5 Fun Facts You Need to Know < http://heavy.com/tech/2017/06/notpetya-petya-ransomware-attack-virus-patch-petrwap-victims/>, retrieved 25.9.2017.

Craiger, P. (2017) Technology, Organizations, and Work in the 20th Century. <http://www.siop.org/tip/backissues/tipjan97/craiger.aspx>, retrieved 20.1.2017.

D'Arcy, J. – Herath, T. – Shoss, M. (2014) Understanding Employee Responses to Stressful Information Security Requirements: a Coping Perspective. *Journal of Management Information Systems,* Vol 31 (2), 258-318.

El-Den, J. – Pham, H. – Richardson, J. (2014) Stress-based Security Compliance Model – an Exploratory Study. *Information & Computer Security,* Vol 24 (4), 326-347.

Eriksson, P. – Kovalainen, A. (2008) *Qualitative Methods in Business Research.* SAGE Publications, Lontoo.

Eskola, J. – Suoranta, J. (1998) *Johdatus Laadulliseen Tutkimukseen.* Vastapaino, Tampere.

Fischer, T – Riedl, R. (2015) Theorizing Technostress in Organizations: A Cybernetic Approach. *In Proceedings of the 12th International Conference on Wirtschaftsinformatik*, Osnabrück, Germany, 1453-1467.

Gartner (2017) Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017, <http://www.gartner.com/newsroom/id/3784965>, retrieved 25.9.2017

Hedström, K. – Kolkowska, E. – Karlsson, F. – Allen, J.P. (2011) Value Conflicts for Information Security Management. *Journal of Strategic Information Systems,* Vol 20, 373-384.

Herath, T – Rao, R. (2009) Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organizations. *European Journal of Information Systems,* Vol 18, 106-125.

Hern, A. – Solon, O (2017) "Petya" Ransomware Attack: What is it and How can it be Stopped? <https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how>, retrieved 25.9.2017

Hoyle, V. (2017) New Rules for Data Protection and Cybersecurity: The Countdown has Started, Will You be Ready? *Credit Control, 38* (1), 19-23.

Hsiao, K. (2017) Compulsive Mobile Application Usage and Technostress: The Role of Personality Traits. *Online Information Review,* Vol 41 (2), 272-295.

Hung, W. – Chang, L. – Lin, C. (2011) Managing the Risk of Overusing Mobile Phones in the Working Environment: a Study of Ubiquitous Technostress. *PACIS Proceedings,* Vol 81, 1-13.

Karjalainen, M. – Siponen, M. (2011) Toward a New Meta-Theory for Designing Information Systems Security Training Approaches. *Journal of the Association for Information Systems,* Vol 12 (8), 518-555.

Krazit, T. (2016) Employees Are the Weakest Link in Computer Security. <http://fortune.com/2016/06/20/employees-computer-security/>, retrieved 30.1.2017.

Lee, A. – Son, S. – Kim, K. (2016) Information and Communication Technology Overload and Social Networking Service Fatigue: a Stress Perspective. *Computers in Human Behavior,* Vol 55, 51-61.

Lee, C. – Lee, C. – Kim, S. (2016) Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity. *Computers & Security,* Vol 59 (2016), 60-70.

Lincoln, Y. S. – Guba, E. G. (1985) *Naturalistic Inquiry*. Sage Publications, Newbury.

Meier, K. (2014) Cybersecurity and Stress – Can Too Much Security be a Bad Thing? <http://www1.udel.edu/udaily/2014/apr/security-stress-042414.html>, retrieved 30.1.2017.

Merriam, S. B. (2014) *Qualitative Research: A Guide to Design and Implementation*. Jossey–Bass, Hoboken. Park, CA.

Murtaugh, P. (2017) The Trials and Errors of GDPR Compliance. < https://www.businesspost.ie/focus-on/trials-errors-gdpr-compliance-397838>, retrieved 22.9.2017.

Okebaram – Moses, S. (2013) Minimizing the Effects of Technostress in Today's Organization. *International Journal of Emerging Technology and Advanced Engineering,* Vol 3 (11), 649-458.

Owusu-Ansah, S, - Azasoo, J. – Adu, I. (2016) Understanding the Effects of Techno-Stress on the Performance of Banking Staff. *International Journal of Business Continuity and Risk Management,* Vol 6 (3), 222-237.

Paavilainen-Mäntymäki, E. (2017) Tutkimusprosessit ja Kvalitatiiviset Tutkimusmenetelmät, harjoitukset. *YSM lectures, spring 2017.* Turku School of Economics.

Patton, M. Q. (2005) *Qualitative Research.* John Wiley & Sons Ltd., New Jersey.

Pirkkalainen, H. – Salo, M. – Makkonen, M. – Tarafdar, M. (2017). Coping with Technostress : When Emotional Responses Fail. *In ICIS 2017: Proceedings of the 38th International Conference on Information Systems,* Seoul, Korea, December, 1-17.

Ragu-Nathan, T. – Tarafdar, M. – Ragu-Nathan, B. – Tu, Q. (2008) The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation. *Information Systems Research*, Vol 19 (4), 417-433.

Saaranen-Kauppinen, A. & Puusniekka, A. (2006) KvaliMOTV - Menetelmäopetuksen Tietovaranto. Tampere: Database of societal studies. <http://www.fsd.uta.fi/menetelmaopetus/kvali/L7_3.html>, retrieved 2.4.2017

Salah-Eddine, M. – Belaissaoui, M. (2016) Technostress, Coping and Job Satisfaction Model of Information Systems. *2016 International Conference on Computational Science and Computational Intelligence,* December, Las Vegas, Nevada, USA, 139-142.

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

Sarajärvi, A. & Tuomi, J. (2009) *Laadullinen Tutkimus ja Sisällönanalyysi.* Tammi, Helsinki.

Savitz, E. (2011) Humans: The Weakest Link in Information Security. <http://www.forbes.com/sites/ciocentral/2011/11/03/humans-the-weakest-link-in-information-security/#44773beb31fd>, retrieved 30.1.2017.

Security Incidents Continue to Rise in Cost and Frequency While Budgets Decrease, according to PwC, CIO and CSO's The Global State of Information Security® Survey 2015. < http://www.pwc.com/us/en/press-releases/2014/global-state-of-information-security-survey-2015.html>, retrieved 30.1.2017

Sellberg, C. – Susi, T. (2014) Technostress in the Office: a Distributed Cognition Perspective on Human-Technology Interaction. *Cognition, Technology & Work,* Vol 16 (2), 187-201.

Shackelford, S. (2017) Exploring the 'Shared Responsibility' of Cyber Peace: Should Cybersecurity Be a Human Right? *Kelley School of Business Research Paper*, 17-55.

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

Spacey, R. – Goulding, A. – Murray, I. (2003) ICT and Change in UK Public Libraries: Does Training Matter? *Library Management,* Vol 24 (1), 61-69.

Speier, C. – Valacich, J. – Vessey, I. (1997) The Effects of Task Interruption and Information Presentation on Individual Decision Making. *ICIS '97 Proceedings of the 18th International Conference on Information Systems,* Atlanta, Georgia, USA, December 1997, 21-36.

Srivastava, S. – Chandra, S. – Shirish, A. (2015) Technostress Creators and Job Outcomes: Theorizing the Moderating Influence of Personality Traits. *Information Systems Journal,* Vol 2015 (25), 355-401.

Stahl, B. – Doherty, N. – Shaw, M. (2012) Information Security Policies in the UK Healthcare Sector: a Critical Evaluation. *Information Systems Journal,* Vol 22, 77-94

Suh, A. – Lee, J. (2017) Understanding Teleworkers' Technostress and its Influence on Job Satisfaction. *Internet Research,* Vol 27 (1), 140-159.

Tak, O. – Park, S. (2016) a Study of the Connected Smart Worker's Techno-Stress. *Procedia: Computer Science,* Vol 91, 725-733.

Tams, S. (2011) The Role of Age in Technology-induced Workplace Stress. *Dissertation presented to the graduate school of Clemson University.*

Tarafdar, M. – Pullins, E. B. – Ragu-Nathan, T.S. (2015) Technostress: Negative Effect on Performance and Possible Mitigations. *Information Systems Journal,* Vol 25 (2), 103-132.

Tarafdar, M. – Tu, Q. – Ragu-Nathan, B. – Ragu-Nathan, T. (2007) The Impact of Technostress on Role Stress and Productivity. *Journal of Management Information Systems,* Vol 24 (1), 301-328.

Tarafdar, M. – Tu, Q. – Ragu-Nathan, T.S. – Ragu-Nathan, B. (2011) Crossing to the Dark Side: Examining Creators, Outcomes, and Inhibitors of Technostress. *Communications of the ACM,* Vol 54 (8).

Tarafdar, M. – Tu, Q. – Ragu-Nathan, T.S. (2010) Impact of Technostress on End-User Satisfaction and Performance. *Journal of Management Information Systems,* Vol 27 (3), 303-334.

Tu, Q. – Wang, K. – Shu, Q. (2005) Computer-Related Technostress in China. *Communications of the ACM – Transforming China,* Vol 48 (4), 77-81.

Viswanath, V. – Morris, M. (2000) Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence, and their Role in Technology Acceptance and Usage Behavior. *MIS Quarterly,* Vol 24 (1), 115-139.

Wang, K, Shu, Q. (2008) *In Proceedings of the 19th International Conference on Database and Expert Systems Applications,* September 2008, Turin, Italy, 420-424.

Yang, L. – Che, H. – Spector, P. (2008) Job Stress and Well-being: an Examination from the View of Person-Environment Fit. *Journal of Occupational and Organizational Psychology*, Vol 81, 567-587.

Young, K. (2004) Technostress. *GPSolo*, Vol 21 (7), 54-55.

APPENDIX 1 – INTERVIEW QUESTIONS

Name:
Organization:
Position/Job title:
Number of years working at the organization:

Background:

1. Can you tell me what types of information security practices you employ in your work?
2. Can you describe what types of information security practices are expected of you in your work?
3. How would you describe your confidence-level regarding your information security skills?
4. How would you describe your feelings/attitude towards your organization's information security policy?

Theme: SRS and the social environment (conflict & news)

5. What reactions do reports about information security gaps in your work or in the technologies you use stir in you?
6. What reactions do reports about information security incidents – for instance the ransomware attacks of the summer – cause in you?
7. Have there been instances in your working life where you've had a conflicting situation between what is in the information security policy and what is expected of you by a boss or a colleague? Can you describe the situation?
8. Is there any stigma in your organization about people who strictly follow information security rules?
9. How do you react when a security warning or a software update pops up in your computer screen?

   Theme: SRS and the personal environment (invasion of privacy)
10. Is your organization monitoring your information security behavior? **If yes:** How does that make you feel? **If not:** How would you feel if your organization would monitor your information security behavior?
11. Have you ever felt as though your organization is invading your privacy by controlling your information security behavior? Can you describe the situation?

Theme: SRS and the work environment (complexity, overload & uncertainty)

12. Have you ever worried about unintentionally causing a security breach in your work? Can you describe the situation?

13. Do you ever feel as though your organization's information security policy & procedures are difficult to understand or time-consuming? In what way?
14. Do the information security practices of your organization increase your workload? Can you describe how?
15. Do you feel as though there are constant changes in the information security practices of your organization? What kinds of changes? How do you react to these changes?
16. How do you/your organization prepare for big information security updates or policy changes (ie. the GDPR)?

Theme: Preventing and reducing SRS

17. What could make you feel more confident about your information security skills?
18. What would you wish to be changed in the information security policy to make it easier or more encouraging?
19. How would you like the information security policy and practices to be communicated to you?
20. How do you feel about information security training? Can you describe what sort of trainings – if any – your organization organizes? Are these trainings effective/what would make them better?