Have We Thought This Through? Understanding the Role of SETA Programs in Mitigating Security-Related Stress (SRS) Creators

Jalal Sarabadani

Department of Management, Information Systems, and Entrepreneurship

Carson College of Business, Washington State University

jalal.sarabadani@wsu.edu

Robert E. Crossler

Department of Management, Information Systems, and Entrepreneurship

Carson College of Business, Washington State University

rob.crossler@wsu.edu

John D'Arcy

Department of Accounting and MIS

University of Delaware

jdarcy@udel.edu

Proceedings of 2020 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop.

Have We Thought This Through? Understanding the Role of SETA Programs in Mitigating Security-Related Stress (SRS) Creators

Research-in-Progress (early stage)

Abstract

Current research in security-related stress (SRS) recommends security education, training and awareness (SETA) programs as an effective way to mitigate the adverse impacts of SRS among individuals, yet this broad assertion has not been unpacked in terms of the underlying mechanisms that connect SETA programs to SRS. Contrary to the conventional wisdom that instructional support and training reduce the destructive effects of stressors, we argue that the inherent characteristics of SETA programs incorporate costs in addition to benefits. More specifically, in this paper, we theorize the underlying mechanisms through which SETA programs provide employees with benefits, costs and their subsequent influence on perception of SRS creators. We expect that the results of this research-in-progress advances our understanding of SETA programs and the way they influence employees' perception of SRS creators, which have been overlooked in the current research. The expected research and practical implications are also discussed in the paper.

Keywords: SETA programs, SRS, security-related stressors, security education, training, awareness

Introduction

Mandatory information security training has been difficult to deal with. The training takes time from my busy schedule and delays my work. I'm required to do it on the clock and by a certain date. Sometimes, I have to go to class to bring myself up to it. I find it to be a burden and time consuming. -- Scott, sales, and marketing expert

I really loved the training sessions I attended. They perfectly fulfilled my needs. I feel like I am more capable of protecting my personal and organizational assets, what a relief! -- Sarah, accounting assistant

The security messages are everywhere and driving me crazy. I receive too many e-mails from IT department. I even see notifications on my mobile phone and even worse, security notifications and pop-ups are coming from every corner of my laptop screen. -- Jack, HR expert

The security requirements were vague to me until the company started to communicate the importance of them, what they mean and why we should care about them. I am happy that I am more flexible to adapt myself with such changes as I am aware of their importance. -- Max, business development manager

As a chief information security officer (CISO), James and his team felt to have found a perfect solution to address the recent issue of employees' feeling of stress due to organization's information security requirements. Now after two months of implementing a comprehensive SETA program and scrolling through the feedback from employees, James is looking even more confused by seeing a mix of positive and negative comments, asking himself: How can this much of training and thorough instructions make these people feel even more stressed?

The above excerpts from conversations with employees at various organizations illustrate a set of interconnected phenomena regarding organizational information security efforts. To protect their digital assets against internal and external threats, companies invest significant amounts of money, time, and energy to implement information security policies (ISPs). ISPs aim to inform employees of the formal procedures, guidelines, roles, and responsibilities required to safeguard and properly use of organizational information technology resources (Lowry et al. 2015). Despite these efforts, research shows that data breaches and other security incidents are on the rise (Willison and Warkentin 2013; Burns et al., 2019; Cram et al., 2019) with employee behavior commonly being identified as a root cause (Cram et al. 2019).

One explanation is the extra burden security requirements stemming from ISPs impose on employees, which at some point becomes taxing, demanding, and exceeding their abilities to deal with them, resulting in feelings of stress (D'Arcy et al. 2014). D'Arcy and colleagues (2014) showed that ISPs can contribute to stress in three ways, which they called security-related stress (SRS) creators. First, SRS-overload is when ISPs increase employees' workload, which forces them to work faster and longer. Lack of permission to specific software programs or certain websites are of such examples. Second, SRS-complexity is experienced when ISPs are usually linked with technical terms and jargon, which are difficult for employees to comprehend and understand. VPN configuration by employees is one example. Lastly, SRS-uncertainty refers to the situation that organizations continuously update their ISPs, which require employees to constantly keep up and adapt with the changing requirements that does not allow employees to establish a base of experience that is unsettling. Frequent changes in the list of websites or applications that employees can use may become frustrating. Although research in SRS is scant, the overall message from the current state of knowledge highlights the different ways SRS results in the violation of ISPs.

To combat this issue, prior research regularly recommends security education, training and awareness (SETA) programs to enhance employees' knowledge and skills, thereby, reducing the complexities and ambiguities associated with ISP-related security requirements (D'Arcy et al. 2009; Lee et al. 2016; D'Arcy and Teh 2019). But do the gains from SETA programs also come with costs? Contrary to the conventional wisdom that more knowledge is better (i.e. literacy facilitation as a technostress inhibitor) (Ragu-Nathan et al. 2008), we argue that the security context is unique in a way that employees are not willing to follow ISPs as they are perceived to be an impediment to their primary work, which adds extra burden. Despite their benefits, this can show that SETA programs also have a dark side that might not be readily apparent. For example, using multiple methods of delivery (in-person vs. IT-enabled), employees are exposed to an endless streams of security related mobile notifications, e-mails, internal newsletters, task reminders, system pop-ups and many more items that interrupt and direct employee's attention from their primary tasks (Addas and Pinsonneault 2015, 2018; Chen and Karahanna 2018). Furthermore, not only the mandatory nature of SETA programs takes employees' time away from their day-to-day job but also increases the learning demand, adaptation requirements and cognitive processing, which are likely to add even more burden to the existing pressure experienced from complying with ISPs.

Prior research in SRS recommends SETA programs as an effective way to reduce SRS among individuals, yet this broad assertion has not been unpacked in terms of the underlying mechanisms that connect SETA programs to SRS. The examples at the beginning of this article highlight that while SETA programs bring about numerous benefits for employees, it is accompanied with costs. To state it more broadly, much of the information security literature

has attempted to highlight the role of SETA by answering "what SETA can do for you?" in the context of information security compliance (Cram et al. 2019) but has been understudied in the context of SRS. Consequently, our understanding of the potential dark side of SETA programs, in terms of the burden they place on employees, is limited. Against this backdrop and relying on several theoretical perspectives from information security and dark side of IT, we develop a research model that explains the mechanisms through which SETA programs positively and negatively influence the perception of SRS in organizations.

This paper makes several contributions to both research and practice. First, to the best of our knowledge, this is the first research endeavor that theoretically and empirically investigates the role of SETA in SRS literature. The research identifies different benefits and costs linked with SETA programs that affect the perception of SRS, which challenges the taken-for-granted assumption that SETA programs mitigate SRS. Not only do we explain how SETA programs reduce the perception of SRS but we also demonstrate how they aggravate the perception of SRS too. Second, this research echoes a broader message to both information security and technostress literature that organizational trainings which are not central to employees' regular job can potentially result in adverse and unexpected consequences as well. We also inform practice by showing the different ways mediating mechanisms triggered by SETA programs can be beneficial or harmful in managing perceived SRS in organizations, so that they can identity these mechanisms first and then leverage the positive effects and weaken the negative effects. Therefore, this research aims to answer the following research questions:

1. *What are the benefits and costs of SETA programs in organizational environments?*
2. *In what ways do these SETA-mediated benefits and costs influence the perception of security related stress (SRS) creators?*

The rest of the paper is organized as follows. In the following section, we present the literature review on SRS and SETA programs. Next, we develop the research model and hypotheses. Then, we present our research method, along with our findings and discussion. Finally, we conclude by highlighting the research and practical contributions of the paper, its limitations, and future directions.

Literature Review

Security-Related Stress (SRS) Research

To explain why ISPs are violated in organizations, D'Arcy and colleagues (2014) contextualized technostress creators in the context of information security and named it security-related stressors (SRS). SRS has been broadly defined as information security demands that create stress in individuals. They present three main factors that are major sources of stress among employees in relation with ISPs in organizations.

SRS-overload describes a situation where ISPs force employees to expend more time and effort to accomplish work-related tasks, hence they should work faster and longer. Such examples are when individuals do not have administrative access to install needed software programs or have limited access to the internet or certain websites. These policies can create hiccups during their work hours and extends their work loads. SRS-complexity is related to the situation where security requirements are complicated and contain complicated technical terms and jargon which are typically difficult to understand and comprehend for employees, hence more time and effort needed to learn about such policies. An example is when employees are required to use certain encryption techniques before sending classified e-mails. SRS-uncertainty

describes a situation when security requirements frequently change, and employees are required to adapt themselves with such changes. A common example is that organizations frequently update the blacklist of software of website that employees are not allowed to use. One consequence of such changes is that employees are required to constantly adapt themselves with security policy changes, which is unsettling for them (D'Arcy et al., 2014).

Although scant number of research papers exists as this is a relatively new area of research, SRS literature can be classified into three broad categories. The first group of studies are the ones that focus on identifying the demands from security policies that are perceived to be stressful by individuals. The second group of studies focus on the direct influence of SRS creators on individuals and the last group of studies focus on the coping strategies individuals take to deal with SRS.

Regarding the first group, D'Arcy and colleagues contextualized technostress creators (D'Arcy et al., 2014) and introduced three major stressors from security demands that we explained in the previous paragraph. Following the work of Ayyagari et al. (2011), Lee and colleagues (2016) introduced work-overload and invasion of privacy as factors that create stress in individuals due to security requirements. Work-overload is equivalent to SRS-overload, but they defined invasion of privacy as tight monitoring practices over employees' ISP compliance activities, which raises privacy concerns such as monitoring over employee's BYOD devices and concerns about their personal information. In a construct development study, Ament and Haag (2016) extended the prior conceptualization by introducing three dimensions of work environment, personal environment, and social environment as potential manifestations of security-related stress creators as a second-order construct. Social environment including conflict and news were the only new dimensions that were added as new security related stressors. They defined conflict as a stressor when there is conflict between security requirements and peers' (managers and colleagues) requests. Stress is likely to arise when individuals are in dilemma to either violate the policies or confront the conflict with colleagues. News was defined as stress individuals perceive from reading or hearing about security-related breaches. Their results showed that social environment stressors motivate individuals to comply with information security policies. Two more studies used qualitative methodologies to identify security related stressors in specific contexts. Savoli et al. (2017) found that unauthorized access to data was the main security related stressor in the context of healthcare. Finally, using multiple interviews from professional employees of multiple organizations (a bank, a university and an oil industry company), Pham et al. (2016) listed access to security policies, security compliance overload and knowledge demand to comply with IT security requirements as demand that are stressful for them. Consistent with prior research and considering it as the leading work in SRS literature, we use D'Arcy and colleagues' (2014) conceptualization of SRS to investigate this phenomenon in our study.

In the second group of studies, Hwang and Cha (2018) examined the effects of SRS on security-related role stress and employees' commitment to the organization. The study showed that individuals with higher levels of SRS experience more security related role stress in the form of role ambiguity and role conflict. A further explanation is that security requirements in a company can be on the way of employees' primary tasks and hinder them from achieving their goals (e.g. paperwork requirements to access an organizational document that might take a few days to get permission), which is likely to create a conflict between one's job goal and organization's security goal. D'Arcy and Teh (2019) investigated the role of discrete emotions, namely fatigue and frustration, in explaining how individuals perceive SRS. Drawing upon

affective event theory, the authors showed that feelings of fatigue and frustration are likely to arise when individuals perceive security demands as taxing. Their findings highlighted that events that hinder employees' primary task attainment (in this case SRS creators) evoke negative emotions in individuals. Lastly, relying on the job-demand control model of stress, Pham et al. (2016) showed that security demands such as overload associated with security compliance and knowledge demand to comply with such policies put a lot of burden on them and create a sense of exhaustion, which subsequently affects their behavior towards ISP compliance.

Finally, the third category of research in SRS are those that have mainly focused on the coping strategies individuals use to deal with the effects of SRS creators. In two related studies, moral disengagement theory (D'Arcy et al. 2014) and neutralization theory (D'Arcy and Teh 2019) were used to explain the different ways employees justify their non-compliant behavior because of SRS creators. Furthermore, in a pure qualitative study in the context of healthcare, Savoli and colleagues (2017) explained that individuals with medical and administrative positions employ multiple coping strategies (e.g. problem solving, negotiation, submission etc.) to deal with stressors from security policies. Table 1 provides a summary of the literature in SRS.

Table 1 summary of the findings in SRS literature

categories / author	Security related stress (SRS) creators	Coping mechanism	Outcomes of interest (direct and indirect effect of SRS)	SETA recommended
D'Arcy et al. (2014)	SRS-overload SRS-complexity SRS-uncertainty	Moral disengagement	Intention to violate ISP	YES
Lee et al. (2016)	Work-overload Invasion of privacy	N/A	Information security stress	YES
Ament and Hang (2016)	Work environment Personal environment Social environment	N/A	ISP compliance intention	YES
Pham et al. (2016)	Access to ISPs Compliance overload Knowledge demand	N/A	Security compliance burnout Security engagement Security compliance	YES
Savoli et al. (2017)	Unauthorized access to data	Multiple coping responses	N/A	NO
Hwang and Cha (2018)	SRS-overload SRS-complexity SRS-uncertainty	N/A	Security-related role stress Organizational commitment Compliance intention	YES
D'Arcy and Teh (2019)	SRS-overload SRS-complexity SRS-uncertainty	Neutralization	Discrete negative emotions ISP compliance	YES

Three observations can be made regarding SRS research. First, due to the prevalent use of ISPs in almost all industries for the purpose of protecting organizational digital assets, researchers have invested time and energy to identify context-specific security-related stressors. Even though D'Arcy and colleagues (2014) were the first to develop SRS creators, emerging research is advancing our understanding of other context-specific types of security related stressors (Savoli et al. 2017). Second, identifying how individuals deal with security related stressors is attracting more attention. This has important implications for both practice and research as it shows the different methods individuals use to confront with SRS and justify their non-compliant behavior. Lastly, which is the interest of this paper, is that there is little to no research paper investigating the mitigation mechanism that reduces the effects of SRS, which

has been highlighted as an important area of research in technostress (Sarabadani et al. 2018; Tarafdar et al. 2019). Specifically, as is evident in Table1, almost all papers indicate that SETA programs are the effective solutions to reduce the destructive impacts of SRS yet left it at the recommendation level.

SETA Programs

Security education, training, and awareness (SETA) programs refer to information security related educational practices that organizations conduct to raise their employees' awareness, knowledge, and skills related to information security topics (D'Arcy et al. 2009). SETA programs are usually ongoing efforts that intend to accomplish several objectives. First, they intend to convey knowledge about risks associated with organizational digital assets. Second, inform employees of their responsibilities to protect organizational resources and lastly actions against security policy violations (D'Arcy et al. 2009). SETA programs can be delivered at three primary levels: awareness only, which largely focuses on "what" threats exist. These awareness programs can be in different formats such as newsletters, e-mails, messages, talks and others. Training (training and awareness) programs are more concerned with "how" of ISPs and usually include practical workshops, hands-on trainings and case studies that show employees how to have a secure behavior in an organizational environment. Lastly, educational programs (education, training and awareness) refer to the practices that deal with "why" threats exist and why having a secure behavior is important in an organizational environment (Crossler and Bélanger 2009; Lowry et al. 2015). To put them in a real example, awareness programs regarding a password policy can explain different threats associated with weak passwords. Training programs can show how to avoid using weak passwords. Finally, educational programs can explain why it is important to avoid using weak passwords.

Classification of prior studies

Prior research in SETA has looked at this phenomenon from different perspectives. Our review revealed two broad categories. First and the most common category includes papers which concentrated on the behavioral effects of SETA and its relation with popular security related phenomena such as IS misuse and computer abuse (D'Arcy et al. 2009; D'Arcy and Hovav 2009; Lowry et al. 2015), ISP compliance (Abdul Talib and Dhillon 2015; Hovav and Putri 2016; Han et al. 2017; Hwang et al. 2017; Burns et al. 2018); security tool usage (Crossler and Belanger 2009), secure behavior (Jenkins and Durcikova 2013) and intention to violate ISPs (Barlow et al. 2018; Herath et al. 2018). Our review of behavioral research showed that all studies followed positivist philosophical view as these papers can be characterized by assuming reality as being objectively given, independent of the observers, quantitatively measurable and using formal hypotheses to test their theories (Myers 2019). The second group of studies had a critical view of SETA programs and papers were more associated with the introduction and development of theory-driven approaches to SETA programs (Puhakainen and Siponen 2010; Karjalainen and Siponen 2011; Goode et al. 2018; Alshaikh et al. 2019). Our research is in line with positivism philosophy and its views to the world and the nature of research in this paradigm, thus, we position our work in the positivism paradigm as well. For the rest of the literature review, we mainly focus on prior literature on behavioral side of SETA to inform our research model development. Table 2 provides a summary of SETA literature in the IS discipline.

Table 2 Summary of prior findings in SETA research

Area of focus	Philosophical view	SETA influence	Authors	Direct influence of SETA (mediator)	Final DV of interest	Results
Behavioral side of SETA	Positivism	Promoting ISP compliance	Burns et al. (2018)	Security valence Security Instrumentality Security expectancy	Intentions to comply with ISP Intentions to protect organizational information assets	SETA → security valence (+) SETA→ security instrumentality (+) SETA→ security expectancy (+)
			Abdul Talib and Dhillon (2015)	Psychological empowerment	ISP compliance intentions	SETA→ psychological empowerment (+)
			Hovav and Putri (2016)	Perceived responses efficacy (PRE)	Intention to comply	BYOD SETA→ PRE (+)
			Crossler and Belanger (2009)	NONE	Security tool usage	awareness→ security tool usage (ns) education → security tool usage (+)
			Han et al. (2017)	Perceived benefits	Compliance intention	SETA→ PB (+)
			Hwang et al. (2017)	Security system anxiety Non-compliance behavior of peers (NCBOP)	Compliance intention	Education → security system anxiety (-) Education → NCBOP (-)
			Jenkins et al. (2013)	Perceived behavioral control (PBC) Attitude toward behaving securely Subjective norms of behaving securely	Intentions to behave securely Secure behavior	Training→ PBC (+) Training → Attitude (+) Training → subjective norm (ns) Just-in-time-reminder → secure behavior (+)
		Discouraging ISP violating	D'Arcy and Hovav (2009)	NONE	IS Misuse intention	SETA → unauthorized access (-) SETA → unauthorized modification (ns)
			D'Arcy et al. (2009)	Perceived certainty of sanctions (PCS) Perceived severity of sanction (PSS)	IS misuse intention	SETA →PCS (+) SETA→ PSS (+)
			Lowry et al. (2015)	Could: external control Would: freedom restriction	Reactive computer abuse	SETA→ external control (-) SETA→ freedom restriction (-) SETA→ Explanation adequacy (+)

				Should: explanation adequacy		
			Herath et al. (2018)	Moral disengagement Policy awareness	ISP violation likelihood	SETA→ Moral disengagement (ns) SETA→ Policy awareness (+)
			Barlow et al. (2018)	NONE	Information security policy violation intention (ISPVI)	SETA informational communication →ISPVI (+) SETA normative communication → ISPVI (ns) SETA anti-neutralization communication → ISPVI (s)
		Costs of SETA	Hovav and Putri (2016)	Perceived response cost	Intention to comply	BYOD SETA→ Perceived response cost (+)
			Han et al. (2017)	Perceived cost	Compliance intention	SETA→ perceived cost (+)
			Hwang et al. (2017)	Work impediment	Compliance intention	Education → work impediment (ns)
Conceptual, development and design of SETA	Interpretivism and critical	Features, components, and approaches to SETA	Puhakainen and Siponen (2010)	N/A	N/A	The paper proposes a training program that are theory-driven and empirically tested using action research methodology. The results suggest that content and methods should be utilized to activate learners' cognitive processing during training.
			Karjalainen and Siponen (2011)	N/A	N/A	The authors developed a new meta-theory to design IS security training approaches to differentiate IS security training from other types of trainings. Their meta-theory introduces four pedagogical requirements for designing any IS security approaches.
			Goode et al. (2018)	N/A	N/A	Using a Delphi method and interview with 21 subject-matter experts, the authors intended to understand what SETA program should encompass.
			Alshaikh et al. (2019)	N/A	N/A	The authors argue that the current SETA programs are not effective and introduce theory-informed SETA development process to overcome the prior shortcomings.

Of the behavioral SETA-related papers, we noticed three observations. The first observation was related to studies that theorized SETA to promote ISP compliance in organizations. Using an experimental research, Crossler and Belanger (2009) examined the

effects of security awareness and education on groups of students and found that those who received security education had a higher use of security tool usage. This is while the effect of security awareness was not significant, about which they concluded that individuals need more instructional support to use security tools. Using a similar methodology, Jenkins and Durcikova (2013) showed that training and just-in-time reminders have a positive influence on individuals to have a secure behavior as it increases their confidence in their abilities and forms their attitude towards adopting a secure behavior. The other related groups of studies primarily used a survey methodology to investigate the different ways SETA programs encourage individuals to comply with ISPs. In the context of Bring-Your-Own-Device (BYOD), Hovav and Putri (2016) highlighted the importance of BYOD-related SETA programs and showed that SETA programs will give employees the confidence that taking secure actions with regard to their BYOD devices (such as smartphones) impedes threats, thereby increases their willingness to comply with ISPs in their organizations. Relying on rational choice theory, Han and colleagues (2017) hypothesized that the benefits employees receive form SETA programs encourage them to comply with ISPs. The result of the study demonstrated that SETA programs help individuals to work in a secure environment and inform them of the potential threats and vulnerabilities, hence they are more aware, acquire necessary knowledge and skills to avoid such threats, and are more motivated to follow ISPs. There were also other studies in which SETA programs encouraged ISP compliance through reduction of security related anxiety and non-compliance behavior of peers (Hwang et al. 2017), increasing psychological empowerment (Abdul Talib and Dhillon 2015), increasing the perception of security valence, instrumentality and expectancy (Burns et al. 2018).

The second category was related to studies which focused on the ways SETA programs affected individuals to avoid malicious activities such as IS misuse, computer abuse, and intention to violate ISPs. For instance, earlier SETA related studies showed that SETA programs reduce individuals' intention to misuse IS in the form of unauthorized access (D'Arcy and Hovav 2009). In a more comprehensive study, D'Arcy and colleagues (2009) explained that those with higher awareness of SETA programs have a higher perception of the severity and certainty of sanctions associated with violating ISPs in the organization, therefore are less inclined to misuse IS. Furthermore, by focusing more on the "why", "how" and "what" framework of SETA programs, Lowry and colleagues (2015) demonstrated that employees will gain more security related knowledge, understand why such ISPs are implemented and they are expected to follow them. SETA initiatives will also help employees to better understand that their company has a control on its information security, hence organizational trust is increased, which subsequently lowers computer abuse. Using a scenario-based survey, Herath and colleagues (2018) also indicated that individuals with higher perception of SETA programs are more aware of security policies in the organization. Therefore, they are less motivated to use rationalization techniques such as moral disengagement to violate ISPs. Lastly, relying on the theory of information communication and using a factorial survey, Barlow et al. (2018) found that different methods of SETA communication (informational and anti-rationalization) reduces the likelihood of violating ISPs as the consequences of violating organizational ISPs are cleared described to employees.

The last observation, which was scarce but important, focused on the relationship between SETA programs and costs associated with them. There were two studies hypothesizing that SETA can have costs for employees and one hypothesizing that security education can lower the perceived cost in the form of reduced work impediment. In their study, Hovav and Putri

(2016) argued that BYOD related awareness and educational programs require employees to do additional procedures on their personal electronic devices, hence their perception of cost is increased. Finding a statistically significant result, they also admitted that the perception of costs might be due to the context as employees are the owner of BYOD devices and should follow the procedures on their personal devices by themselves. In line with the previous research, similar result was concluded by Han and colleagues (2017), who indicated that SETA programs are positively associated with perceived costs of compliance such as work impediments. However, contrary to the previous studies, Hwang et al. (2017) argued that SETA programs reduce individual's work impediment although they did not provide a clear justification of how SETA programs reduce employees' work impediment. After all, their results did not support their hypothesis.

Overall, studies on SETA programs inform us in several ways. First, SETA programs are effective to promote employee's compliance behavior with organizational ISPs. Furthermore, they can also be served as effective tools to discourage employees to violate ISPs by increasing their awareness of the consequence of such violations, enhancing their knowledge and skills. Lastly, recent research shows that SETA programs come with costs too. This is an important finding indicating that even though security-related programs boost employees' knowledge, the nature of such programs (e.g. mandatory and ongoing) (D'Arcy et al. 2009; Puhakainen and Siponen 2010) might be a source of conflict with individuals' primary and daily tasks. However, research in the costs associated with SETA programs are limited and inconclusive. More specifically, it is unclear in what ways features and characteristics of SETA programs incur cost on employees and in what forms such costs appear.

SETA programs and SRS research

As stated earlier in the SRS literature, there has been very few theoretical and empirical attempts to reduce the negative effects of SRS in organizations. Meanwhile, our literature review of SRS showed that almost all papers encourage organizations to implement SETA programs, mainly to increase and boost employees' awareness, knowledge, and skills as a remedy to the detrimental effects of SRS creators. Furthermore, our literature review from SETA programs revealed that even though the majority of literature in SETA programs have highlighted the positive effects on promoting ISP compliance behavior and reducing ISP violation behavior, literature has started the argument that SETA programs may be a source of overhead and burden too.

While SETA programs have common characteristics with other organizational forms of training, they can be distinguished in some ways. For instance, most of the SETA programs are mandatory as ISP violations occur despite an individuals' job title (Puhakainen and Siponen 2010). Second, SETA programs are offered in many different formats such as face-to-face training sessions, hands-on experiences, online courses, or even informational messages using traditional methods such as newsletters, flyers, and newer methods like e-mail and mobile notifications, reminders, screen pop-ups and others (Crossler and Bélanger 2009; Jenkins and Durcikova 2013; Hovav and Putri 2016; Herath et al. 2018). These have shown to be a major source of interruption at work, which demand more cognitive processing time from individuals and shift their attention from one task to another that is costly (Chen and Karahanna 2018; Tams et al. 2020). Lastly, even though SETA programs are recommended to be repetitive and ongoing (D'Arcy et al., 2009), over exposure to SETA related programs (from receiving awareness messages on the phone to participating security related education courses) can

negatively influence individuals and deprive them from doing their primary tasks at the surface, resulting in the perception of more stress.

Being informed by the previous studies and based on characteristics of SETA programs, we develop a theoretical model that explains the underlying mechanisms SETA programs mitigate or aggravate the perception of SRS creators. To be able to theorize both positive and negative implications of SETA programs in the context of security-related stress, we draw upon multiple theoretical views to explain how major characteristics and features of SETA programs mitigate or aggravate the perception of SRS among employees. The outcomes from SETA characteristics can influence the perception of SRS creators in different ways. In the next section, we theorize how such outcomes influence SRS creators. Table 3 shows different outcomes from SETA characteristics and how their effects are reflected on SRS creators.

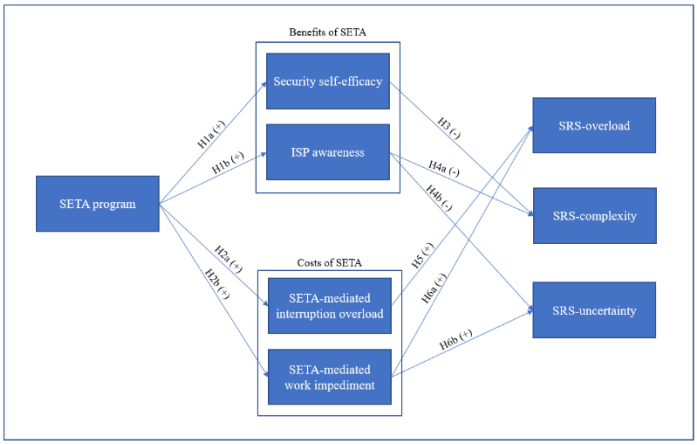
Table 3 benefits and costs associated with SETA in relation with SRS creators

SETA characteristics and features	Type of outcome	expected outcome in the form of cost-benefit	reflection of outcomes on SRS creators		
			SRS-overload	SRS-complexity	SRS-uncertainty
Enhanced knowledge and skills	positive	security Self-efficacy		✓	
Communication of ISPs	positive	Policy awareness		✓	✓
Frequency	negative	SETA-mediated interruption overload	✓		
		SETA-mediated work impediment	✓		✓
Mandatory	negative	SETA-mediated work impediment	✓		✓
Methods of delivery	negative	SETA-mediated work impediment	✓		✓
		SETA-mediated interruption overload	✓		
Content update	negative	SETA-mediated work impediment	✓		✓

Research Model and Hypotheses Development

Figure 1 shows research model of the study. In this model, SETA programs are associated with both positive outcomes (security self-efficacy and ISP awareness) and negative outcomes (SETA-mediated interruption overload and SETA-mediated work impediment). Furthermore, the model demonstrates that the associated costs and benefits influence different aspect of SRS creators.

Figure 1 research model



SETA programs aim to achieve two broad objectives: First, to make sure employees are aware and understand information security policies that are in place in their organizations (D'Arcy et al. 2009). To reach this goal, such programs are implemented at three levels of awareness, training, and education to answer the questions of "what", "how" and "why" of ISPs and threat associated with them (Crossler and Bélanger 2009). Training employees about ISP-related threats from different angles fulfills employees' need of knowledge about ISPs and threats (Alshaikh et al. 2019), hence employees are more confident about their capabilities regarding ISPs (Jenkins and Durcikova 2013).

Prior research has shown that individuals who received security related trainings felt higher levels of knowledge acquisition and were more confident to take necessary actions to have a safe behavior in their company (Jenkins and Durcikova 2013; Hovav and Putri 2016). The second objective of SETA is to communicate these policies with employees to remind them of the ISPs in their organizations, their roles and responsibilities and highlight the importance of these ISPs. Barlow and colleagues (2018) showed that different forms of SETA communication such as informational, social and anti-neutralization communication will inform employees of the ISPs in organizations and how a company treats those who violate ISP, which subsequently will increase the perception of their awareness related to existing ISPs from different angles. Similar results were found by Herath and colleagues (2018) that frequency of communication allows employees to have higher awareness of organizational ISPs. Therefore, in line with prior research we propose the following hypotheses, which articulate benefits of SETA programs:

H1a: SETA programs are positively associated with security self-efficacy.

H1b: SETA programs are positively associated with policy awareness.

While SETA programs bring about considerable benefits for employees, they have potential costs too (Hovav and Putri 2016; Han et al. 2017). One of the distinguishing features of SETA programs is that they are usually mandatory (Puhakainen and Siponen 2010). This is because ISPs are set at the organization level and despite employees' expertise, they are required to follow such policies. However, from employee's point of view, SETA programs are on the way of their primary tasks (Bulgurcu et al. 2010). Moreover, research has shown that employees see ISPs as a barrier to their work and are not willing to follow (Bulgurcu et al. 2010), meaning that any other activities related to ISPs give them similar feelings. For instance, Hovav and Putri (2016) showed that BYOD-related SETA programs require employees to follow different security related procedures to make sure that their devices meet organizational ISP requirements. In addition, SETA programs use a variety of methods to deliver contents and cover a wide range of ISP related topics.

SETA programs can adversely influence individuals in a variety of ways due to their inherent characteristics. Research in SETA literature has widely pointed to online and traditional modes of content delivery as benefits of SETA programs, but it has ignored the fact that these methods of content delivery and communication can also be a source of interruption to individuals' primary work (Addas and Pinsonneault 2015; Tams et al. 2020). Such interruptions can appear in the form of e-mail and mobile notifications, messages, pop-ups and many more (D'Arcy et al. 2009; Jenkins and Durcikova 2013; Crossler and Belanger 2009). Moreover, prior research has supported the idea of repetition of such methods of delivery to ensure SETA programs are effective (Herath et al. 2018). While it might be true, we argue that over exposure of employees to ISP related educational materials will give them a higher

perception of overload from SETA-mediated interruptions. In their interruption framework, (Speier et al. 2003) highlighted interruption frequency, duration, content, complexity, and timing of are cognitive dimensions of interruption tasks that influence primary tasks. Lastly, in addition to being mandatory and causing interruption, SETA programs frequently present employees with updates about new policies, new data breach events, instructions to avoid those threats, the reasons behind threats and many more. This takes significant amount of cognitive processing from individuals, adaptation, and learning flexibility. Therefore, SETA programs can feed employees with too much information, which becomes on the way of handling their regular job. Hence, we hypothesize that:

H2a: SETA programs are positively associated with SETA-mediated interruption overload.

H2b: SETA programs are positively associated with SETA-mediated work impediments.

According to social cognitive theory (SCT) (Bandura 1977), self-efficacy refers to one's judgement of her/his ability to perform a certain behavior. Drawing upon SCT, (Compeau and Higgins 1995) introduced the concept of computer self-efficacy to refer to a person's judgement of their belief to use a computer. There is a rich body of literature indicating that individuals with higher computer self-efficacy are likely to show higher levels of performance and lower levels of computer anxiety (Compeau and Higgins 1995; Venkatesh et al. 2003). Furthermore, in a similar fashion, the concept of computer self-efficacy has been adapted in the security domain based on the argument in the literature that computer self-efficacy needs to be context specific (Crossler 2010).

Based on prior literature, we define security self-efficacy as one's judgement of her/his ability (skills, knowledge, or competency) to protect organizational IS assets from internal and external threats (Bulgurcu et al. 2010; Crossler 2010). Rich body of literature in information security has supported the positive link between self-efficacy and a secure behavior. For instance, Bulgurcu and colleagues (2010) demonstrated that employees with higher ISP related self-efficacy are more likely to comply with the organizational ISPs. Furthermore, Crossler (2010) showed that individuals with higher security self-efficacy gain more confidence in their ability to secure their devices and are more likely to frequently backup their data.

In the context of SRS, we argue that individuals with higher levels of security self-efficacy not only learn technical terms related to security threats, but also learn how to avoid those threats. The enhanced security related knowledge increases their confidence and competence to identify threats even without the help of others. Moreover, these people can identify threats that are new to them as they are familiar with such threats and have gained confidence in their abilities to protect themselves against threats (Shahri et al. 2016). Moreover, technostress literature shows that people with higher perception of self-efficacy are more eager to learn new skills rather than to resist (Shu et al. 2011). Similarly, individuals with higher security self-efficacy are more eager and likely to engage with IPSs to protect themselves and organizational assets against potential threats. This means that employees are more receptive to learn technical terms and jargon, which makes the perception of understanding organizational ISPs less difficult, frustrating and stressful for them. Therefore, we hypothesize that:

H3: Security self-efficacy is negative associated with SRS-complexity.

ISP awareness refers to an individual's understanding of organizational ISP requirements and the goals of those security requirements (Herath et al. 2018). Information security literature has noted that individuals who are aware of their organizational ISPs have a better understanding of benefits associated with following those ISPs and costs linked with violating them. For instance, Herath and colleagues (2018) and D'Arcy et al. (2009) showed that those who are aware of ISPs in the organization have a clearer understanding about the consequences of violating such ISPs, thus are less likely to violate ISPs by rationalizing their risky behavior. Furthermore, relying on rational choice theory, Bulgurcu and colleagues (2010) demonstrated that higher levels of security awareness is positively associated with complying with security policies in the organizations. This is mainly because such a behavior brings them benefits that make them feel satisfied, fulfilled, rewards such as being praised by peers and colleagues in the company and the feeling that their resources are safe.

In the context of SRS, we argue that employees' awareness of ISPs helps them in several ways. First, ISP awareness will eliminate ambiguities about organizational expectations related to ISPs. we argue that employees who are aware of ISPs in their organizations, have a better understanding of the nature of those policies, how those policies are related to them and their responsibilities towards them. This results in lower levels of ambiguity about ISPs, which is a source of stress among individuals (Tarafdar et al. 2007; Ragu-Nathan et al. 2008; Sarabadani et al., 2020). Second, employees with higher perception of ISP awareness are more likely to adapt themselves with organizational security policy requirements. For instance, Herath et al. (2018) demonstrated that employees who are aware of the ISPs in their organizations, are more willing to be engaged in taking pro-security behaviors. One explanation for this behavior is that awareness changes employees' beliefs and cognitive processing about ISPs (Bauer and Bernroider 2017). This can also imply that they are more receptive to the upcoming and new changes of ISPs as they have a good understanding of the benefits and values of those ISPs for them and the organization. Therefore, we hypothesize that:

H4a: ISP awareness is negatively related to SRS-complexity.

H4b: ISP awareness is negatively related to SRS-uncertainty.

Interruptions have been defined as "uncontrollable, unpredictable stressors that produce information overload, requiring additional decision-make effort" (Speier et al. 2003, p.772). Interruptions are external events that create attentional conflicts between the demands from the interruption and primary tasks (Addas and Pinsonneault 2015). Drawing upon the theories of distraction conflict theory (DCT), relevant research has advanced our understanding of the many ways through which interruptions can impact individuals' performance, such as the frequency, duration, content and form of interruptions (Speier et al. 2003). Moreover, several other relevant studies indicated that interruption requires immediate attention and action from individuals (McFarlane and Latorella 2002), which subsequently influence their decision-making performance (Speier et al 2003) leading to the appraisal of the interruptions as a source of stress (Galluch et al. 2015).

In a similar vein, IT-mediated interruption has been defined as "perceived, IT-based external events with a range of content that captures cognitive attention and breaks the continuity of an individual's primary task activities." (Addas and Pinsonneault 2015, p.233). Based on our review of SETA and cognitive dimension of interruption tasks, we argue that SETA programs can aggravate the perception of SRS. We specifically argue that features of SETA programs such as frequency, methods of delivery and variety of contents create a situation

where individuals are prone to too many interruptions from SETA initiatives that are facilitated by e-mail and mobile notifications, reminders, pop-up messages and many more. Chen and Karahanna (2018) describe this phenomenon as interruption overload, which refers to perceived overload caused by interruption. Building on Chen and Karahanna (2018), We define SETA-mediated interruption overload as the extent to which users receive more interruptions than they can effectively process and handle due to SETA programs.

In the context of IT and according to (Addas and Pinsonneault, 2015), three main characteristics of IT can facilitate IT-mediated interruption. First, IT-mediated interruptions are usually accompanied by a notification alert. Common examples are notification sounds and pop-up messages that appear on individuals' digital devices. The second feature is parallelism that enables individuals to handle multiple interactions at the same time. And the last feature is repeatability which allows individuals to shift their attention form the primary task and engage themselves with the content of the interruption.

In the context of IT-mediated interruption, Addas and Pinsonneault (2018) showed that exposure to incongruent e-mails that are irrelevant to the primary tasks increases individuals' perception of overload that subsequently lowers their performance. Similarly, knowing that employees work with many applications and more than one digital device (such as desktop computers and BYOD devices), they are more likely to receive many awareness, training and educational messages through different methods of communications such as e-mail and mobile notification, system pop-ups and many more of other items, which directs their attention away from their primary tasks. Switching attention from one to another task increases the cognitive load on individuals' mind that results in lower performance and inability to continue primary tasks (Tams et al. 2020).

Furthermore, as employees work with multiple applications using different devices, they are likely to be exposed to significant number of awareness, training, and educational messages. While some of these contents might only be informational, some require employees' action to follow procedures to comply with organizational policies (addas and Pinsonneault 2015). Not only do these take their attention away, but also require cognitive processing (Speier et al. 2003). Such instances are password policy e-mail interruptions, which takes employees' attention via a notification alert on their digital devices and shift their attention to a non-primary task and demands cognitive processing from individuals by giving instructions on how to change their passwords. Over exposure to these interruptions will dampen employees' ability to focus on their primary tasks, that subsequently reduces their work performance as similar results have been found in the IT-interruption literature (Chen and Karahanna, 2018). Thus, we propose that:

H5: SETA-mediated interruption overload is positively associated with SRS-overload.

Work impediment has been defined as a detriment to an individuals' primary task because of complying with security requirements in the company. Literature states that compliance with ISPs consumes considerable amount of time and effort from employees' day-to-day job that negatively influences their performance at work (Bulgurcu et al. 2010). In the context of BYOD, Hovav and Putri (2016) showed that compliance with IPSs incur both physical and cognitive load on employees, leading to the higher perception of costs of complying with policies. Likewise, in a different study, Han and colleagues (2017) showed that security tasks are on the way of employees' primary job in many ways such as interrupting their work, slowing

down their device or making them completely out of use, which are likely to lead to the perception of higher workload and result in lower levels of productivity.

In line with prior research, we define SETA-mediated work impediment as detriments to an employees' daily tasks due to the requirements from SETA initiatives. We argue that SETA-mediated work impediments can affect employees in several ways. For instance, SETA training and education sessions require employees to participate in talks, discussions, workshops, and hands-on training sessions. In addition to sacrificing their working time to participate in such classes, they also require employees to spend time and effort to practice the instructions they receive, which are perceived as time-consuming and a significant barrier to the accomplishment of their tasks, thus resulting in higher perception of workload. Moreover, as new threats and data breaches are reported, new ISPs are implemented, which means new training sessions to employees. The continuous adaptation and learning demand from these training programs are unsettling and uncomfortable to employees. Thus, we propose the following hypotheses:

H6a: SETA-mediated work impediment is positively associated with SRS-overload

H6b: SETA-mediated work impediment is positively associated with SRS-uncertainty.

Research Methodology

The primary goals of this paper are to understand the benefits and costs of SETA programs and how they influence employees' perception of SRS. Therefore, a field study methodology deems an appropriate approach to answer the research questions of this study. Our intention is to provide a snapshot of the different ways through which SETA programs influence SRS. This research will specifically use survey as it is common in field studies because surveys are suitable methodologies to capture data from various respondents with different demographic information such as age, gender, education, work, experience, industry and others to provide a generalized understanding of this phenomena.

Sample

The population of our interest for this study will be ICT users, broadly defined. The study population includes employees of organizations who use technology (e.g. desktop computers, laptops, and smartphones) frequently in their job and work as a full-time employee. To get responses from the right people, we will ask two screening questions. First, whether they are aware of the presence of ISPs in their organization. Second, if they have received SETA related programs in the past 6 months. To sample from this population, we will use a national survey panel (e.g. Qualtrics), an aggregator of market research panels. Qualtrics will send the survey to a random selection of panel members living in the USA, who are above 18 years old and full-time employees.

Online market research panels are appropriate to distribute the survey to our target sample of the population for several reasons. First, online market panels allow us to collect data from large population of respondents (Steelman et al. 2014). Second, online research panels provide access to respondents with different backgrounds and experiences. Third, the screening options allow us to approach respondents who are a proper fit to our research (Lowry et al. 2016). Finally, online panels provide built-in anonymity and features to ensure data quality (Rouse 2015).

Measures

Measures of the construct will be taken from the existing literature. More specifically, SETA programs will be taken from D'Arcy et al. (2009). Security self-efficacy, ISP awareness and SETA-mediated work impediment will be taken from Bulgurcu et al. (2010) and adapted appropriately to this research. SETA-mediated interruption overload will be adapted from Chena and Karahanna (2018). SRS creators will also be taken from D'Arcy et al., (2014). Table 4 in Appendix 1 shows the list of measures, which will be used in this study. Items will be measured on a 5-point Likert scale from 1 being strongly disagree and 5 being strongly agree.

Procedures

Qualtrics will send the invitations to the respondents. Potential panelists will be directed to click on our survey link where they will read a consent form describing the research and then decide whether to proceed with the survey. Attention check questions will be included in the survey, asking respondents to click a specific response if they are reading the question. If a participant does not answer the attention check questions correctly, the survey will be terminated, and the response will be discarded.

Analysis and Results

To make sure our data is of high quality, we will follow procedures suggested by Burleson et al. (2019). In their paper, the authors proposed a framework, known as "5-c framework", which provides guidelines to authors on the primary aspects of data quality and procedures that IS researchers need to follow before, during and after data collection, when using a survey methodology.

To assess the psychometric properties, we will follow Straub and colleagues (2004). To test the reliability of the constructs, we will check Cronbach's alpha and composite reliability according to recommendation from the literature (Straub et al. 2004). To test the validity of the constructs, we will conduct convergent and discriminant validity tests. For convergent validity, we will calculate Average Variance Extracted (AVE). Values for all constructs should be above the minimum required threshold of 0.5 (Segars 1997) to show convergent validity is met. To test discriminant validity of the constructs, we will check the cross-loadings of the items. We will also use Fornell and Larcker test and check if the squared root AVEs of all constructs are greater than the correlation between themselves and other constructs. Finally, we will use Heterotrait-Monotrait (HTMT) ratio of correlations criterion as a further analysis to make sure that the constructs are discriminant (Henseler et al. 2015). A cut off value of .85 as a reference shows the constructs are discriminant. After establishing the validity of the constructs, we will test the research model using path modelling techniques, implemented in SmartPLS 3.2.6 to explain the variance, significance, and direction of the relationship between constructs (Ringle et al. 2015).

Contribution to Research and Practice

This study is expected to contribute to research and practice in several manners. First, we theorize the different ways that inherent characteristics of SETA programs can lead to both positive and negative outcomes. This research will extend prior SETA studies by stating that SETA programs can have dark side by overloading employees with ISP-related educational interruptions and hindering them from accomplishing their primary tasks.

Second, to the best of our knowledge, this will be the first study to theoretically and empirically incorporate SETA programs in the context of SRS. This paper contributes to the current literature by challenging the existing belief that training reduces technostress. More

specifically, we hope to provide evidence that training programs, in this case SETA programs, can have adverse effects, and aggravate the perception of SRS among employees.

We will also contribute to practice by highlighting the following points. First, this study will inform information security managers that SETA programs have potential to negatively influence individuals. Therefore, when designing and implementing SETA programs, they should pay close attention to the fact that such educational programs can be major sources of interruption and increase employees' workload, if not properly designed. Moreover, this paper sends the message that while SETA programs can be used as mitigators of SRS creators by increasing their security self-efficacy and ISP awareness, the perception of SRS-overload and uncertainty might be aggravated through SETA-mediated interruption overload and work impediment. This highlights that managers should give considerable thought on factors such as the frequency, method of delivery, type of content they deliver to reduce the costs of SETA programs on employees' side.

References

Abdul Talib, Y. and G. Dhillon (2015). "Employee ISP compliance intentions: an empirical test of empowerment."

Addas, S. and A. Pinsonneault (2015). "The many faces of information technology interruptions: a taxonomy and preliminary investigation of their performance effects." Information Systems Journal 25(3): 231-273.

Addas, S. and A. Pinsonneault (2018). "E-mail interruptions and individual performance: is there a silver lining?" MIS quarterly 42(2): 381-406.

Alshaikh, M., H. Naseer, A. Ahmad and S. B. Maynard (2019). "Toward sustainable behaviour change: An approach for cyber security education training and awareness."

Ament, C. and S. Haag (2016). "How Information Security Requirements Stress Employees."

Ayyagari, R., V. Grover and R. Purvis (2011). "Technostress: technological antecedents and implications." MIS quarterly 35(4): 831-858.

Bandura, A. (1977). "Self-efficacy: toward a unifying theory of behavioral change." Psychological review 84(2): 191.

Barlow, J. B., M. Warkentin, D. Ormond and A. Dennis (2018). "Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance." Journal of the Association for Information Systems 19(8): 3.

Bauer, S. and E. W. Bernroider (2017). "From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization." ACM SIGMIS Database: the DATABASE for Advances in Information Systems 48(3): 44-68.

Bulgurcu, B., H. Cavusoglu and I. Benbasat (2010). "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness." MIS quarterly 34(3): 523-548.

Burleson, James; Carter, Michelle; and Sarabadani, Jalal, "On the importance of data quality in information systems research and ph.d. curricula" (2019). 2018 Proceedings. 18.

Burns, A., T. L. Roberts, C. Posey, R. J. Bennett and J. F. Courtney (2018). "Intentions to comply versus intentions to protect: A VIE theory approach to understanding the influence of insiders' awareness of organizational SETA efforts." Decision Sciences 49(6): 1187-1228.

Chen, A. and E. Karahanna (2018). "Life interrupted: The effects of technology-mediated work interruptions on work and nonwork outcomes." MIS quarterly 42(4): 1023-1042.

Compeau, D. R. and C. A. Higgins (1995). "Computer self-efficacy: Development of a measure and initial test." MIS quarterly: 189-211.

Cram, W. A., J. D'arcy and J. G. Proudfoot (2019). "Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance." MIS quarterly 43(2): 525-554.

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. 2010 43rd Hawaii International Conference on System Sciences, IEEE.

Crossler, R. E. and F. Bélanger (2009). "The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage." Journal of Information System Security 5(3).
D'Arcy, J., T. Herath and M. K. Shoss (2014). "Understanding employee responses to stressful information security requirements: A coping perspective." Journal of Management Information Systems 31(2): 285-318.
D'Arcy, J., A. Hovav and D. Galletta (2009). "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach." Information systems research 20(1): 79-98.
D'Arcy, J. and A. Hovav (2009). "Does one size fit all? Examining the differential effects of IS security countermeasures." Journal of business ethics 89(1): 59.
D'Arcy, J. and P.-L. Teh (2019). "Predicting employee information security policy compliance on a daily basis: the interplay of security-related stress, emotions, and neutralization." Information & Management.
Galluch, P. S., V. Grover and J. B. Thatcher (2015). "Interrupting the workplace: Examining stressors in an information technology context." Journal of the Association for Information Systems 16(1): 1.
Goode, J., Y. Levy, A. Hovav and J. Smith (2018). "Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness." Online Journal of Applied Knowledge Management (OJAKM) 6(1): 54-66.
Han, J., Y. J. Kim and H. Kim (2017). "An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective." Computers & Security 66: 52-65.
Henseler, J., Ringle, C. M., and Sarstedt, M. (2015). A New Criterion for Assessing Discriminant Validity in Variance-based Structural Equation Modeling., Journal of the Academy of Marketing Science, 43(1): 115-135.
Herath, T., M.-S. Yim, J. D'Arcy, K. Nam and H. R. Rao (2018). "Examining employee security violations: moral disengagement and its environmental influences." Information Technology & People.
Hovav, A. and F. F. Putri (2016). "This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy." Pervasive and Mobile Computing 32: 35-49.
Hwang, I. and O. Cha (2018). "Examining technostress creators and role stress as potential threats to employees' information security compliance." Computers in Human Behavior 81: 282-293.
Hwang, I., D. Kim, T. Kim and S. Kim (2017). "Why not comply with information security? An empirical approach for the causes of non-compliance." Online Information Review.
Jenkins, J. and A. Durcikova (2013). "What, I shouldn't have done that?: The influence of training and just-in-time reminders on secure behavior."
Karjalainen, M. and M. Siponen (2011). "Toward a new meta-theory for designing information systems (IS) security training approaches." Journal of the Association for Information Systems 12(8): 3.
Lee, C., C. C. Lee and S. Kim (2016). "Understanding information security stress: Focusing on the type of information security compliance activity." Computers & Security 59: 60-70.
Lowry, P. B., J. D'Arcy, B. Hammer and G. D. Moody (2016). "'"Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels." The Journal of Strategic Information Systems 25(3): 232-240.
Lowry, P. B., C. Posey, R. J. Bennett and T. L. Roberts (2015). "Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust." Information Systems Journal 25(3): 193-273.
McFarlane, D. C. and K. A. Latorella (2002). "The scope and importance of human interruption in human-computer interaction design." Human-Computer Interaction 17(1): 1-61.
Myers, M. D. (2019). Qualitative research in business and management, Sage Publications Limited.
Pham, H.-C., J. El-Den and J. Richardson (2016). "Stress-based security compliance model–an exploratory study." Information & Computer Security.
Puhakainen, P. and M. Siponen (2010). "Improving employees' compliance through information systems security training: an action research study." MIS quarterly: 757-778.
Ragu-Nathan, T., M. Tarafdar, B. S. Ragu-Nathan and Q. Tu (2008). "The consequences of technostress for end users in organizations: Conceptual development and empirical validation." Information systems research 19(4): 417-433.

Ringle, C. M., S. Wende and J.-M. Becker (2015). SmartPLS 3. Boenningstedt: SmartPLS GmbH
Rouse, S. V. (2015). "A reliability analysis of Mechanical Turk data." Computers in Human Behavior 43: 304-307.
Sarabadani, J., Carter, M., & Compeau, D. (2018). 10 Years of Research on Technostress Creators and Inhibitors: Synthesis and Critique.
Sarabadani, J., Compeau, D., & Carter, M. (2020). An Investigation of IT Users' Emotional Responses to Technostress Creators. In Proceedings of the 53rd Hawaii International Conference on System Sciences.
Savoli, A., S. Addas and I. Fagnot (2017). "Coping with Information Security Stressors in Healthcare."
Segars, A. H. 1997. "Assessing the Unidimensionality of Measurement: A Paradigm and Illustration within the Context of Information Systems Research," Omega (25:1), pp. 107-121.
Shahri, A. B., Z. Ismail and S. Mohanna (2016). "The impact of the security competency on "self-efficacy in information security" for effective health information security in Iran." Journal of medical systems 40(11): 241.
Shu, Q., Q. Tu and K. Wang (2011). "The impact of computer self-efficacy and technology dependence on computer-related technostress: A social cognitive theory perspective." International Journal of Human-Computer Interaction 27(10): 923-939.
Speier, C., I. Vessey and J. S. Valacich (2003). "The effects of interruptions, task complexity, and information presentation on computer-supported decision-making performance." Decision Sciences 34(4): 771-797.
Steelman, Z. R., B. I. Hammer and M. Limayem (2014). "Data collection in the digital age: Innovative alternatives to student samples." Journal of Consumer Psychology 23(2): 212-219.
Straub, D., Boudreau, M., and Gefen, D. 2004. "Validation Guidelines for IS Positivist Research," The Communications of the Association for Information Systems (13:1), pp. 63.
Tams, S., M. Ahuja, J. Thatcher and V. Grover (2020). "Worker stress in the age of mobile technology: The combined effects of perceived interruption overload and worker control." The Journal of Strategic Information Systems 29(1): 101595.
Tarafdar, M., Q. Tu, B. S. Ragu-Nathan and T. Ragu-Nathan (2007). "The impact of technostress on role stress and productivity." Journal of Management Information Systems 24(1): 301-328.
Tarafdar, M., Cooper, C. L., & Stich, J. F. (2019). The technostress trifecta-techno eustress, techno distress and design: Theoretical directions and an agenda for research. Information Systems Journal, 29(1), 6-42.
Venkatesh, V., M. G. Morris, G. B. Davis and F. D. Davis (2003). "User acceptance of information technology: Toward a unified view." MIS quarterly: 425-478.
Willison, R. and M. Warkentin (2013). "Beyond deterrence: An expanded view of employee computer abuse." MIS quarterly: 1-20.

Appendix 1

Table 4 Measurement items

Constructs	Items	Citation
SETA Programs	My organization provides training to help employees improve their awareness of information system security issues.	D'Arcy et al., (2009)
	My organization provides employees with education on computer software copyright laws.	
	In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.	
	My organization educates employees on their information system security responsibilities.	
	In my organization, employees are briefed on the consequences of accessing information systems that they are not authorized to use.	
Security self-efficacy	I have the necessary skills to fulfill the requirements of the ISP.	Bulgurcu et al., (2010)
	I have the necessary knowledge to fulfill the requirements of the ISP.	
	I have the competencies to fulfill the requirements of the ISP.	
	I know the rules and regulations prescribed by the ISP of my organization.	Bulgurcu et al., (2010)

ISP awareness	I understand the rules and regulations prescribed by the ISP of my organization.	
	I know my responsibilities as prescribed in the ISP to enhance the IS security of my organization.	
SETA-Mediated Interruption Overload	During regular working hours, I feel overload because I receive more interruption from information security related trainings and awareness message (via e-mail, computer, mobile etc.) than I can process	Chen and Karahanna (2018)
	During regular working hours, I feel rushed frequent interruptions I receive more interruption from information security related trainings and related awareness messages (via e-mail, computer, mobile etc.).	
	During regular working hours, I feel busier because I must handle interruptions from information security related trainings and related awareness messages (via e-mail, computer, mobile etc.).	
	During regular working hours, I feel pressure due to interruptions from information security related trainings and related awareness messages (via e-mail, computer, mobile etc.)	
	During regular working hours, the number of work-related interruptions I receive from information security related trainings and related awareness messages (via e-mail, computer, mobile etc.) exceeds my ability to handle them.	
SETA-Mediated Work impediment	Security education, training and awareness programs in our organization holds me back from doing my actual work	Bulgurcu et al., (2010)
	Security education, training and awareness programs in our organization slows down my response time to my colleagues, customers, managers, etc.	
	Security education, training and awareness programs in our organization hinders my productivity at work	
	Security education, training and awareness programs in our organization impedes my efficiency at work	
SRS-overload	I am forced by information security policies and procedures to do more work than I can handle.	D'Arcy et al. (2014)
	My organization's information security policies and procedures hinder my very tight time schedules.	
	I have a higher workload due to increased information security requirements.	
	I am forced to change my work habits to adapt to my organization's information security requirements.	
SRS-complexity	I sometimes feel pressure in my job due to information security requirements	D'Arcy et al. (2014)
	I find that new employees often know more about information security than I do.	
	I do not know enough about information security to comply with my organization's policies in this area.	
	I often find it difficult to understand my organization's information security policies.	
	It takes me awhile to understand my organization's information security policies and procedures.	
	I sometimes do not have time to comply with my organization's information security policies	
SRS-uncertainty	There are constant changes in information security policies and procedures in my organization	D'Arcy et al. (2014)
	There are frequent upgrades to information security procedures in my organization.	
	There are always new information security requirements in my job.	
	There are constant changes in security-related technologies in my organization.	