Discussion of Technostress Impact on Employees' Information Security Behaviour

Masterarbeit

zur Erlangung des akademischen Grades „Master of Science (M.Sc.)“ im Masterstudiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Sokolowski Vorname: Linda

[redacted] [redacted] [redacted] [redacted]

Prüfer: Prof. Dr. M. H. Breitner

Hannover, den 30.Oktober 2017

Table of Contents

1 Introduction

The high level of digital connectivity, powered by innovations in information systems, has a transformative effect on the way information is accessed, processed and stored (Dinev & Hu 2007, p. 387). Rapid changes in the application and usability of information and communication technologies (ICTs) such as networking technologies have facilitated new types of global information sharing (Bloom et al. 2014, p. 2859). Information plays a crucial role in supporting an organization's business operations and encouraging an organization to achieve a competitive advantage over others (Posthumus & von Solms 2004, p. 639). While information is valuable and considered to be one of the important assets of an organization, it is also vulnerable to a variety of attacks from both inside and outside of organizations such as hackers, viruses, and data losses, etc. All the security risks can cause actual and potential losses with financial, legal, and reputational impacts (Culnan et al., 2008, p. 50; Straub & Welke 1998, p. 442). Therefore, information security is a crucial strategic part of the key priorities of the organizational management (Tu & Yuan 2014, p. 1). In order to reduce the risk of information security breaches, organizations tend to use technological solutions and neglect the human risk factor (Bulgurcu et al. 2010, p. 524). Previous scholars stated that the mere use of technological measures is not enough to sufficiently achieve information security since the majority of security breaches originate from inside the organizations (Siponen & Vance, 2010, p. 487; Vroom & von Solms, 2004, p. 193). According to the aforementioned studies, employees ignoring compliance with basic security procedures can be a greater security threat than cybercriminals (Dimensional Research 2014, p. 8). For this reason, literature often refers to employees as the weakest link in the information systems (IS) security chain. This in turn reinforces the importance of implementing a strong combination of technology and employee security awareness throughout a company (Ifinedo 2012, p. 84). In general, organizations provide information security policies which contain essential behavioural rules and guidelines in order to ensure a safe handling of information while performing their everyday tasks (D'Arcy et al. 2014, p. 286; Bulgurcu et al. 2010, p. 524). Difficulties arise when employees are unaware of such ISP or uncertain in handling the measures included in the policies (Karjalainen et al. 2013, p. 519). The non-IT-related resource which contains the compliance of information security policies by employees is subject to growing interest in practice and research. Although, developing guidelines and policies is an important starting point, it is not enough to ensure employees' compliance with them (Bulgurcu et al. 2010, p. 524). Therefore, an understanding of which determinants influence and drive employees to comply with their organizations' information security requirements is essential to diagnose the deficiencies in their information security management efforts (Bulgurcu et al. 2010, p. 524).

On the other hand, organizations have gained significant benefits of the use of ICTs, such as improvements in performance and productivity, as well as extensive possibilities for communication (Melville et al. 2004, p. 285). Despite this positive influence, organizational use of ICTs becomes increasingly complex, ubiquitous, functionally pervasive, challenging, often requiring employees to process information simultaneously and continually from different devices and applications. (Tarafdar et al. 2010, p. 304; Ragu-Nathan et al. 2008, p. 417). Consequently, employees spend as much as 28% of their working time dealing with

interruptions from multi-tasking mainly due to ICT, which results in significant psychological costs, negative emotions and attitudes (Brillhart 2004, p. 304). Employees are increasingly frustrated and overwhelmed by continued efforts required to cope with new applications, functionalities and workflows due to the pervasiveness of ICTs, and resulting in so-called technostress (Tarafdar et al. 2010, p. 304; Tarafdar et al. 2011, p. 114). Because this study focuses on employees as the major risk factor, it is also important to shed more light on employees with their individual differences. The aim of this thesis is to identify determinants of technostress, which (indirectly) influence employees' security compliance intention, and identify the cognitive beliefs and factors influencing individual's intention. Furthermore, the aim is to examine the role of personality traits in this context. For this purpose, theories from different research fields are used in the present study.
The foundation for this study is represented by the Theory of Planned Behaviour (TPB) (Ajzen 1991), the Transaction-Based Model of Stress (McGrath 1976, Lazarus and Folkman 1984, Cooper et al. 2001), and the Big Five personality traits comprising the Five-Factor Model (FFM) (e.g. Barrick et al. 2001; Judge et al. 2002). Prior scholars emphasize the impact of technostress on the individual's attitudes, beliefs and behaviours caused by the ICT, and may be perceived differently depending on the dominant personality traits of the individuals which in turn influence certain job outcomes (Srivastava et al. 2015, p. 357), such as job satisfaction, which can act as an important antecedent of security compliance intention (D'Arcy & Greene 2014, p. 483). Furthermore, the construct of self-efficacy of the TPB was confirmed in prior research regarding the positive influence on employees' security behavioural intention (e.g. Herath & Rao 2009, p. 117; Bulgurcu et al. 2010; Johnston & Warkentin 2010). This study does not only contribute valuable research to prior information security studies but also gives valuable insights to technostress research, as well as personality research. For the following research question, a research model was developed and empirically analysed:

RQ: *How does technostress influence employees' information security compliance intention, and do personality traits play a significant role?*

The study is structured as follows: In Chapter 2, the present state of research is shown. Furthermore, information security and technostress are explained. The chapter ends with a presentation of the underlying theories (Transaction-Based Model of Stress, TPB and FFM), as well as certain overlaps between the Transaction-Based Model of Stress and TPB are given. Based on these findings hypotheses are developed in Chapter 3 which is followed by the research methodology in Chapter 4. In Chapter 5, the data analysis and results of this study are represented. The result section is separated into results from the measurement model analysis and results from the structural equation modeling (SEM). Afterwards, the results are discussed in Chapter 6. Limitations are discussed in Chapter 7. Finally, conclusion and further research are shown in Chapter 8.

which may have a combined and interactive impact on the perception if technostress creators and thus have varied effects on job satisfaction. This study is using a nomothetic approach, which is also the prevalent approach in occupational stress literature and widely accepted for examining the moderating effect of personality traits on the relationship between stressors and job outcome (Grant & Langan-Fox 2006; Srivastava et al. 2015, p.).
The study is influenced by other factors which have not been taken into account. For example the hierarchy structure within the organization could be a possible factor. It can be assumed that flat hierarchies enable a better information flow, whereas the employees have the possibility to communicate about their ICT issues and ask for help, which may lead to greater appreciation of the employees. This might improve their identification with their organization. Contrarily, it could be that employees in organizations with less flat hierarchies perceive more technostress because of lower closeness to the management and no quick channels of communication.
Due to those limitations in this research, findings show tendencies but cannot be easily generalized. These can be addressed in future studies.

8 Conclusion and Outlook

The purpose of this present study is to investigate how technostress influence employees' information security behaviour. By using job satisfaction as a mediating variable, the indirect impact of technostress creators on security compliance intention was examined.
Additionally, the study incorporated the significant role of personality traits in this context to emphasize the human factor as a major risk factor with its individual differences. Thereby, the study focuses on the combined influence of personality traits and technostress creators on job satisfaction rather than the direct impact of personalities on technostress.
The research model integrates constructs from the TPB, and Transaction-Based Model of Stress, and is extended with the Big Five personality traits by leveraging the FFM.
The model was tested based on a survey (n=303) with SEM.
Results show that technostress by means of certain technostress creators (techno-insecurity, techno-invasion, techno-overload) has a negative influence on employees' job satisfaction which in turn has a negative impact on their security compliance intention. The negative relation between job satisfaction and security compliance is contrary to the findings of D'Arcy and Greene (2014) and should be further investigated in future.
Moreover, employees were more satisfied with their job, they perceived higher self-efficacy as their beliefs in their ability to comply with the information security requirements of their organization. Also, the positive influence of self-efficacy on security compliance intention was confirmed.
Additionally, the findings prove the moderating influence of personality traits on the relationship between technostress creators and job satisfaction. Respectively, conscientiousness, extraversion, and openness to experience positively moderates the negative relation between technostress creators and job satisfaction, so that these traits can dampen the negative effect of technostress on job satisfaction, whereas neuroticism negatively moderates this negative relationship, and strengthens this negative relation. The fifth personality trait

agreeableness needs to be examined with different items.
In this way, it is important that upcoming studies investigate internal mechanisms that are held by the employees themselves with their individual cognitions and feelings as influential factors in combination to their relative stable personality traits, besides external organizational mechanisms, that can enhance an employee's security compliance behaviour. Associated therewith additional antecedents that influence employees' self-efficacy could be integrated into this model.
Since technostress is mostly associated with negative feelings, it should be taken into account that stress may have the potential to trigger certain behaviours that are necessary to handle a challenging task such as understanding new technology at work in order to fulfill their work tasks, therefore future research should consider the reflective view on technostress and point out the positive mechanisms as well, in relation to security compliance behavior.
Besides, one could consider further mediating variables that link the relation between technostress creators and employees' behavioural intentions towards information security.
Lastly, it could be informative to examine the proposed model cross-culturally and across various industries.