Empirical Case Study of Mobile Technostress Influence on Information Security Behaviour of Employees

Masterarbeit

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

vorgelegt von

Name: Lemke Vorname: Kevin

[redacted] [redacted]

Prüfer: Prof. Dr. Breitner

Hannover, den 05. Juni 2018

Table of Content

List of Tables I
List of Figures III
List of Abbreviations IV
1 Introduction 1
1.1 Study Objective and Research Question 1
1.2 Structural Approach 4
2 State of the Art 5
2.1 Technostress 5
2.2 Mobility and Smartphones 8
2.3 Information Security and Information Security Behavior 10
3 Theoretical Background 19
3.1 Transtheoretical Model of Stress and Coping 19
3.2 Transaction Based Model 23
3.3 Work-Home Interference & Boundary Theory 28
4 Developing the Research Model 31
4.1 Preliminary Thoughts 31
4.2 Theory of Planned Behavior 33
4.3 Defining Information Security 36
4.4 General Description of the Model 37
4.5 Research Model 39
4.6 Development of Hypotheses 40
4.6.1 Definition of Mobile Technostress Outcomes 40
4.6.2 Development of Hypotheses 42
4.6.3 Overview of Hypotheses 51
5 Research Methodology and Quality Criteria 52
5.1 Quantitative Research vs. Qualitative Research 52
5.2 Quantitative Research Objects and Measurement 53
5.3 Quality Criteria for Measurement Models 55
5.4 Survey Setup and Research Design 59
5.5 Operationalization of Indicators and Construct 60
5.6 Illustration of Research Process 63

5.7 Empirical Findings 65
5.7.1 General Findings 65
5.7.2 Testing and Evaluation of Outer Constructs 66
5.7.3 Testing Structural Equation Model 73
6 Discussion of Results 78
6.1 Discussion of Research Hypotheses 78
6.2 Answering the Research Question 87
7 Limitations 89
8 Theoretical and Practical Implementations 92
9 Conclusion 95
References IV
References of Media Pages XII
Appendix XIII

1 Introduction

1.1 Study Objective and Research Question

Nowadays companies have to consider multiple business aspects in order to operate effectively. On one hand, they require physical capital like machines and factories and on the other hand, they require highly educated employees to run their business according to the resource-based view developed by Barney (Barney 1991). Like displayed above, the following research will guide through the topic of technostress, focussing on the mobile aspect of technostress. The second major topic is about information security, investigating how information security is achieved and identifying typical information security threats to present how information security behavior will influence the safety status of information. One major connection between this two concepts is the Theory of Planned Behavior.

Since the introduction of modern ICT, handling information has shifted in multiple dimensions, discussing the idea of storing, processing and transferring data and the protection of information (Heinrich et al. 2014). This transformed handling information into a complex theme with multiple opportunities and multiple risks as well. Hence the optimal use of data and information is one of the major factors to successfully run a modern business (Niederman et al. 1991; Epple et al. 1996; Argote and Ingram 2000; Gordon and Loeb 2002). Information and communication technology has changed the way how business is done dramatically. One major example is the connection of business processes globally through new possibilities of communication and information sharing (Johnston and Vitale 1988; Bensaou and Venkatraman 1996; Dong et al. 2009). On top of this, the implementation of mobile ICT (MICT) should ensure faster business decisions through increased accessibility and connectivity to the organizational information stock and allow easier management of connections to employees on a global scale (Davis 2002). Eventually, the use of ICT has shifted organizational effectiveness to a new level of operation (Matusik and Mickel 2011; Dery and MacCormick 2012). But as a matter of fact, there are not only positive aspects connected to the use of ICT. Besides new possibilities to analyze data, a crucial topic is information security (Hamill et al. 2005; Herath and Rao 2009). The digitalization of information has lead to an easy remote access to the company's information but not exclusively for people with authorized access, if given the skills, outsiders with specialized knowledge about computer systems can gather internal information via remote access too and use them for their personal gains (Whitman 2003; Keeney et al. 2005; Zeadally et al. 2012). There is no need for physical access to the company for information theft (Colwill 2009). People from all over the world have the possibility to disclose data from companies. Organizations need to take necessary steps in order to protect the information from unauthorized access, disclosure, disruption, modification, recording or destruction (Coles-Kemp and Theoharidou 2010; Zeadally et al. 2012; Ifinedo 2012).

That is why organizations introduced general information security practices which should ensure the right behavior for information security and started to implement security policies and software to increase their cyber defenses (Herath and Rao 2009). The damage caused by information security breaches is diverse and ranges from financial loss or loss of intellectual property up to reputational displacements (D'Arcy et al. 2009; Sarker 2010). Organizations usually make large investments in order to keep outsiders away from their information sources and thus underestimating consequences possibily generated by insider violations (Zeadally et al. 2012).

In particular, the following research will investigate one important subject regarding information security, also known as information security behavior. In case information security awareness seems to be a crucial source of harmful information security behavior (D'Arcy et al. 2009). Especially people with low information security awareness may act careless and cause information security breaches unintentionally (D'Arcy et al. 2009). In consequence and with regard Bandura's social cognitive theory of learning this kind of behavior is dangerous towards information security especially in the case of people disregarding policies, because when someone is able to neglect policies without any punishment it is likely that others will adopt the same behavior when it leads to positive personal outcomes (Bandura 1986; Herath and Rao 2009). In addition, the attitude towards the company and its information security seems to be important for organizational success in information security. Often people's intentions are not malicious when causing information security breaches. Moreover, people are often not aware of possible consequences of their actions, thus they act unaware of consequences. For example, surfing privately on companies devices can help an outsider to gain access to the company through viruses or phishing of personal data (Stanton et al. 2005; Herath and Rao 2009). In the end, the amount of financial loss caused by an insider may be as high as from an outsider, but especially information security breaches which are caused by the ethical flexibility of persons need to be prevented (D'Arcy et al. 2009; Zeadally et al. 2012). However, the detection of information security threats from inside is not as easy as from the outside because in general, employees have licensed access to information sources (Sarker 2010). Also organizations fear reputational damage when the public knows that the origin of information security threats is inside the company. Hence technological solutions are not enough to prevent misuse from inside (Sarkar 2010). Above all MICT enable people to work outside the company which allows that information is carried around and makes information security behavior more crucial than ever before (Davis 2002; Derks and Bakker 2014). People are the weakest link in the information security chain (Stanton et al. 2005; Ifinedo 2012). As a result, the research suggests that the use of information and communication technology not only fosters the productivity and performance of a company but also causes problems in uncharted territory (Tarafdar et al. 2011).

One important point of employee behavior is technology-related stress which will be the second big topic of this research. Technology is evolving rapidly with growing demands of the user. Sometimes technological changes make it hard to adapt to a new situation (Adner and Levinthal 2001; Ragu-Nathan et al. 2008). Incidentally, indicators like age, gender and knowledge influence the connection between a user and ICT but ongoing changes might create a fear regressing productivity because of missing technological knowledge (Ragu-Nathan et al. 2008; Shu et al. 2011). Especially MICT have high requirements for time management and creating boundaries in order to separate work from private life. Employees need to create space for family demands whilst having the time for recreation (Galinsky et al. 2001; Derks and Bakker 2014). People feel forced to check their smartphone consistently to answer important emails and messages. Moreover, the social surroundings might create high pressure for answering immediately so in the end especially MICT requires high management actions to prevent an overload in multiple dimensions (Hung et al. 2011; Dery and MacCormick 2012; Derks et al. 2015). The topic of technostress relates to the Transtheortical Model of stress and coping which was developed by Lazarus and Folkman (Lazarus and Folkman 1984, 1987). The topic of stress has been researched widely so that the model is still adequate to describe the creation of stress and possible behavioral outcomes. In recent years organizations started to care more about the origins of stress because of huge individual and organizational turnovers. The individual outcomes are ranging from lack of motivation up to frustration and burnouts and in case of organizational outcomes from lower productivity up to a higher turnover rate (Ragu-Nathan et al. 2008). This leads to a loss of financial and personal gains (Zeadally et al. 2012). To sum it up, technology in general but moreover through the design of more flexible workplaces derived by the evolution of mobile ICT has created a high dependency which, in case of overuse, is the trigger of mobile technostress. In the end, the existence of technostress might not only influence individual and organizational outcomes but might be the origin of bad information security behavior and the cause of information security breaches. So the following research will investigate:

How and why does mobile technostress influence the information security behavior of employees?

1.2 Structural Approach

The following scientific elaboration deals with at least two major aspects, the topic of mobile technostress and the topic of information security. In addition, there will be a focus on information security threats caused by faulty human behavior inside the company. Hence the influence of mobile technostress and their effects on information security behavior will be elaborated. After having introduced the basics, the second chapter will deal with the examination of the status quo of recent research. There will be an elaboration of mobile ICT, information security, technostress and theoretical aspects of behavioral psychologic to provide the basic knowledge for further model development. After having examined the past and important constructs for this research int third part the fourth part deals with the development of the research model and the construction of a research hypotheses. Afterwards, the research design will be explained and researched items will be conducted in chapter five. Also, the fifth chapter is going to present the analysis of the collected data set and in the last general aspects will be presented. In the end, there will be a discussion about whether to neglect or accept the research hypotheses and the general reseach question will be answered. In addition limitations encountered in this thesis regarding theoretical research and data sampling will be adressed in chapter seven. After having discussed the limitations of this work there will be theoretical and practical implications and this project will be concluded with suggestions for future research.

9 Conclusion

This research tried to investigate into the connection between mobile technostress and information security behavior. Based on the theories regarding technostress, Boundary Theory and information security two broad constructs were developed. On the one hand the construct of mobile technostress and outcomes and on the other hand important categories for information security behavior got developed. The Theory of Planned Behavior was used in order to connect both research projects. Through using quantitative research people had to give requests to models indicators by filling in an online questionnaire. After all the entire model got evaluated by using multivariate analytical methods. Despite the construct of mobile technostress was not researched well the empirical results of this research show that mobile technostress definitively exist and especially the construct of technooverload showed huge empirical evidence by showing strong connections to every defined outcome namely “job satisfaction”, “organizational commitment” and “producitivity”. Above all, future research has to keep the focus on mobile technologies because they become more and more powerful and applicable to most tasks in the daily office routine that they are able to replace common ICT and change how and especially at which locations work is done (Siau et al. 2001; Davis 2002; Sarker and Wells 2003). So this research delivered important first insights for possible consequences from working remotely due to MICT. But the amount which could be researched was very limited as there is much more work necessary in order to evaluate the triggers and outcomes more in detail. To sum it up it is important for future research to look into the personal outcomes of mobile technostress even more, as well the mobile technostress trigger constructs with special regard towards WHI. In addition the aim is to identify reliable organizational and personal outcomes in order to implement practical countermeasures.

This research also investigated information security behavior. Recent research investigated a lot in sectors of deterrence strategies like monitoring peoples information system use in order to control their usage behavior and research experimented with using sanctions when employees were acting against the information security rules (D'Arcy et al. 2009; Herath and Rao 2009). In the end these kinds of deterrence strategies could support information security behavior but this empirical research showed other important evidence. The organizational situation of a person with regard to their commitment, job satisfaction does matter in that case because it influences the attitude and perceived behavioral control of a person which are both main drivers for an action of a person regardless which kind of action. In this case slight evidence was found that these constructs are influencing the behavioral intention to follow policies and doing preventive measures against information security breaches on their mobile devices. Thus in the end this is leading to an enormous focus on the person which is the greatest possible risk to information security in companies (Whitman 2003).

It is important to seek for patterns which can rise or diminish the motivation and attitude of people to act in positive information security behavior. In the end when organizations find a way to improve the internal motivation of people and to raise the attitude and awareness of people towards information security threats, people might act in their best way possible for information security on their own and not because they fear to get punished for noncompliance to their company's information security behavior.

Finalized this research delivered a good theoretical basis for further modification and adjustment. This type of research will remain on high importance for future theories and practices because smartphones are more and more used in organizations and this researched showed that accessibility at any time and any place might have negative consequences for information security because behavior which is practiced outside the company cannot get monitored that easy and moreover information are carried around outside the company which makes it even more complicated to protect them against misuse. Thus, this topic is leading to a huge challenge for companies regarding future smartphone use for professional content in regard to information security behavior.