Influence of Risk Preferences Considering Personality Traits on the Information Security Behavior

Masterarbeit

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

vorgelegt von

Name: Breitenstein Vorname: Lars

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

Prüfer: Prof. Dr. Michael H. Breitner

Hannover, den 30.09.2019

Table of Contents

1 Introduction and Motivation

"The own employee's[1] are the most important resource for companies, but also the biggest risk" (Kempf 2016)

One of the greatest challenges for today's companies is the information security. More specifically how personal, organizational and technical factors can work together without neglecting information security (see Hu et al. 2012: 650).
In the new global and digital economy, more and more companies cannot work without the Internet. Employees as well as companies are more and more connected to each other. This facilitates the communication and also accelerates it significantly (see Porter & Heppelmann 2014: 4). In recent years, there has been an increasing interest in "flex at work" also known as mobile work or home-office. That means companies give their employees the possibility to work from home or on their way to the next meeting (see Brenke 2016: 95). Especially for employees with kids or if they have an important appointment this work-model is very popular (see Nansen et al. 2010: 149; Weichbrodt 2014: 2). Therefore the information has to be available from all over the world. This may affect the flexibility and the productivity of the employee in a positive way (see Diaz et al. 2012: 500; Hill et al. 1998: 667), but also affect the companies' security in a negative way (see Nansen et al. 2010: 145; Densham 2015: 5). So the companies offer more space for cyber attacks and this makes the improvement of the security technology as well as the sensitization of their employees very important as (see Spinellis, Kokolakis & Gritzalis 1999: 125ff.).

According to Bitkom, approximate 70% of German companies have been victims of digital attacks in the last two years. Nearly half of them caused damage, which amounts to 43.4 billion euros over the last two years (see Bitkom Research 2018). That shows that security threats can have massive damage for companies. Not only in a financially way. Prestige as well as the credibility of the company can be damaged if the company will be a victim of a cyber crime (see Bulgurcu et al. 2010: 544; D'Arcy & Hovav 2007: 113; Cavusoglu, Mishra & Raghunathan 2004: 69). Researchers, as can see in Appendix 1, estimate that nearly half of data breaches and security violations occur by an employee (see Armstrong 2016; Richardson 2011: 20). This shows that the employees are often the weakest link in the information security system (see Ifinedo 2013: 84; Warkentin, Shropshire & Johnston 2007: 1; Guo et al 2011: 204; Vroom & von Solmes 2004: 193). One reason to underline the statement above is, that people deal with information differently (see

[1] Gender Disclaimer: In order to ensure better readability all terms used in this paper refer to female, male and divergent persons.

Warkentin, Shropshire & Johnston 2007: 1; Guo et al. 2011: 204f.). This issue is caused by the different risk preferences as well as personality traits of the employees (see Ewald, Maart & Mußhoff 2012: 159; Uffen, Guhr & Breitner 2012: 12). But the security awareness of the employees has an impact on the security behavior as well (see Cavusoglu, Mishra & Raghunathan 2004: 81; Boss et al. 2015: 51). For example, some employees write down their passwords openly or leave their workstations without locking the computer. Others will open emails from an unknown sender and get infected by open the attachment that includes malware or spyware (see Shropshire, Warkentin & Sharma 2015: 177). So more and more companies try to improve their internal security, like the behavior of their employees (see Anderson & Agarwal 2010: 613).

These cases above show that many security attacks are caused by the violation of the security compliance by internal employee or inattentive actions (see Myyry et al. 2009: 136). Furthermore, it underlines the current relevance of this topic. This paper should study the influence of the risk awareness as well as risk preferences considering personality traits on the information security behavior. The aim of this thesis is to answer the following three questions:

> **How do risk awareness as well as risk preferences influences the information security behavior considering the personality traits of the employees?**

Currently very little is known about the influence of the risk awareness and the risk preferences considering personality traits on the information security behavior. The importance and originality of this study are that it explores the relationship of risk preferences and personality traits to the information security behavior. This is the first study that researches the combination and the relationship between personality traits and risk preferences regarding the information security behavior.

This master thesis should deepen the findings of Mrs Guhr and her colleagues from 2018. They examine the impact of leadership on employees intended information behavior. One of the findings was that younger and older groups of people have different information security behavior (see Guhr, Lebek & Breitner 2018: 352). Based on these results this study gets a deeper research of the effects of risk awareness as well as risk preferences considering personality traits on the information security behavior.

The characterization of information security behavior is very important to increase the security. Furthermore, the study tries to improve the understanding of the employees and offer some methods for the companies how they can increase their security with a special view of the different personality traits and risk preferences of their employees. More over to get an understanding how firms can optimize the security awareness of their employees and reduce the risk of cyber attacks.

The next chapter begins by laying out the theoretical dimensions of this paper. This chapter gives a brief overview of the recent history of the security technology and the role of information for companies. Furthermore, it gives an overlook what information security is about and explains the political point of view (e.g. DSGVO). At the end of this chapter there will be explained the information security management, the risk preferences and the personality traits in general.
This thesis is composed of five themed subchapters at chapter three. In this chapter all the main key words of this study as well as their sub-points will be briefly explained. It begins with the risk awareness and is following by the risk preferences of human beings. It will then go on to the personality traits and the information security behavior. This chapter ends by the derivation of the research design. The fourth chapter is concerned with the methodology used for this study and the fifth section presents the findings of this study. The discussion of the findings as well as the given implication for the future research and for the practice will present in chapter six. At the end of this paper there will be a short conclusion and an outlook.

2 Theoretical Foundations

2.1 The Development and Status Quo of Security Technology

The market place in the todays digital world is for the companies the online marked. So the companies get more and more connected to each other or selling their products online (see Cavusoglu, Mishra & Raghunathan 2004: 69). As a result, companies can work much faster and flexibly, but they also offer more space for cyber-crime (see Gordon, Loeb & Sohail 2003: 81).

In 1983 the first cyber crime was discovered by the FBI. The hacker group "414s" hacked thousands of supposedly secure computer systems in North America and Canada (see Chatfield 2013: 99). Hacking in the sense of cyber crime means that a person gets mostly undetected access to a foreign computer system without any permission (see Hockmann & Knöll 2008: 31). From that moment hacking becoming a trend but here a distinction must be made between the different types of hackers.

Another important practical implication is that schedules or written instructions for work processes could be created so that new employees directly know how to do something or can look again inside if they are unsure. Companies should follow Ifinedo's recommendation (2014: 76) and include regular training and other security-related topics (e.g. regular password changes) in their security compliance.
The results of this study indicate that awareness plays an important role for long-term and effective information security behavior. For this purpose, companies (as mentioned in chapter 3.1) should hire or create a security manager or security department. A reasonable approach to tackle this issue for companies (especially for small companies) could be to hire a security manager of an external company. The security manager, for example, will be in the company once a week and is available for personal security consultation or security questions as well as for paying attention of security breaches (e.g. whether the screen are looked off if the employee is leaving their place). But in long term, this study suggests to having their own security department due to the cost-effectiveness. Moreover the security managers are insiders of the company and know exactly how the security system works. Further the other employees better known the own security manager and that does create more trust. But the development in this area is still positive (cf. Appendix 3). As a result more and more companies are using a DLP security program (see Liebhart 2011: 24). That is an important trend and it is important that the companies don't rest.

The following chapter seven is the final part of this master-thesis. In this chapter the major finding is summarized and the research question is answered. It concludes with a brief look into the future.

7 Conclusion and Outlook

The main reason for this work was the current threat to companies in form of hacker attacks and the fact that more and more data breaches can be attributed to human failure or are only made possible by humans misbehavior (see Bitkom Research 2018; Warkentin, Shropshire & Johnston 2007: 1). The aim of the present research was to examine to what extent risk awareness and risk preferences, considering personality traits, has an influence on the information security behavior. Special about this study was that the personality traits were examined as a moderator for the relationship between risk preferences and information security behavior. Based on risk awareness, risk preferences and personality traits (as moderator), fourteen hypotheses were derived. This has the background that the information security behavior was divided into extra- and in-role behavior. The constructs were measured with the help of a standardized online questionnaire and evaluated with the help of multivariate analysis methods using the SmartPLS program. Thus the present research question could be answered.

The results of this online survey indicate that personality traits do not moderate the relationship between risk preferences and information security behavior. Furthermore, there was no significant effect of the risk preferences on the in- and extra-role behavior of the employees. So far, the first part of the research question can be answered. The most obvious finding to emerge from this study is that the security awareness plays a significant role for information security behavior. The education of employees and the associated security awareness is very important for companies. The incident at the Iranian nuclear power plant in which an employee accidently spread a virus (Stuxnet) by using a USB (cf. chapter 2.1) shall not be repeated. This could have massive consequences for humanity. This underlines the importance of information security and what kind of power the information of companies may be able to have.

Past research has often investigated information security behavior and its influenceability (see Safa & Von Solms 2016; Connolly et al. 2017). Mrs Guhr and her colleagues (2018) disprove the finding that punishment for non-compliance and reward for compliance with security compliance leads to improved information behavior in the long term. Due to the fact, this master-thesis have consider only intrinsic motivation and provides important new insights into how companies can increase employee's motivation to improve information security behavior over the long term. In addition this research show some approaches with which actions the company can increase the security awareness. But it will always be a hard battle between the companies/states and the hackers with the goal of being as secure as possible. In this context much more research is needed, particularly in relation to new technologies such as speech assistants at work or smart devices and their acceptance of employees. Moreover, research in the area of security managers should be intensified in order to find out which characteristics a security expert should have to have a higher influence on the information security behavior of the employees.

Furthermore, it is important for future studies to determine a standard measurement for the risk preferences in order to distinguish the results from others and to suggest a better comparability. In addition further or new possibilities should be found for companies to increase the intrinsic motivation of the employees in the long term. Because the development of new technologies is extremely fast moving it must be noted that what is new today will be old tomorrow. In addition many employees also use company phones and laptops outside the company or the companies offer

BYOD (bring your own device) (see Gupta, Seetharaman & Raj 2013: 865; Diaz et al. 2011: 500; Nansen et al. 2010: 149; Downer & Bhattacharya 2015: 1). A major challenge for the future is that employees have to behave outside the company in a security-compliant behavior in order to protect the company's data as well as possible. As explained in chapter 2.2, IT security not only has an important influence on security against hacker attacks, but also on the continued existence of the entire company (see D'Arcy & Hovav 2007: 113; Hockmann & Knöll 2008: 131; Honekamp 2019: 48).

For this reason a company can only maintain information security at a high level in the long term if employees acquire security-compliant automatisms and explicitly think about possible consequences of their own actions. Due to that the results of this work will be relevant for future research. Against this background and also because personality traits have no moderating effect on the relationship between risk preferences and information security behavior this research forms a good theoretical basis for future modifications and adaptations.

Ultimately the statement of the German former president's Walter Scheel (a. D.) that nothing happens without a risk can be approved. Companies can never completely eliminate risks they can only reduce it. This work has shown which possibilities a company has to reduce the risk (security programs, insurances etc.) and what a company can do to improve information security behavior.

This work has shown that it is today not even necessary to use violence to attack or blackmail someone. Therefore in nowadays a computer is enough (see Hockman & Knöll 2008: 131). To sum up, bits and bytes are the new bullets and bombs. Everyone should be aware of how convenient and simple everyday life with IT is but also of the dangers it entails. It is up to all of us to protect this convenience, even luxury, by being careful with the technology, gaining a better understanding and protecting it.