Empirical Analysis of Leadership and Social Learning Effects on Employees' Information Security Behaviour

Masterarbeit

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

vorgelegt von

Name: Vogel Vorname: Vanessa

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

Prüfer: Prof. Dr. Michael H. Breitner

Hannover, den 19. September 2014

Table of Contents

1. Introduction

Information security represents a topic with increasing interest (Boss, Kirsch, Angermeier, Shingle and Boss, 2009, p. 151). Especially the variety of laws and regulations require the save handling of information and data and force an increased attention towards information security (Warketin, Johnston and Shropshire, 2011, p. 267). Information security regulations are a burden to employees and employer (Warketin et al., 2011, p. 267). Breaching information protection can cause serious consequences for organisations. Its reputation can suffer and information security breaches can cause enormous costs (Warketin et al., 2011, p. 268; Bulgurcu, Cavusoglu and Benbasat, 2010, p. 524; D'Arcy, Hovav and Galetta, 2009, p. 79). Information security is part of the key priorities of the top management. Their interest consists in reducing the risk towards information security (Bulgurcu et al., 2010, p. 524). In order to reduce the risk of information security breaches, organisations tend to use technological solutions and neglect the human risk factor. The mere use of technological solutions is not enough to sufficiently achieve information security because employees represent the major security risk (Bulgurcu et al., 2010, p. 524; Siponen and Vance, 2010, p. 487; Vroom and von Solms, 2004, p. 193). For that reason, it is interesting and important at the same time to examine human behaviour to find out which factors can work affecting in this respect. Normally, organisations provide information security policies which contain essential behavioural rules in order to obtain a save handling of information (D'Arcy et al., 2009; Bulgurcu et al., 2010, p. 524). Problems arise when employees are unaware of such information security policies or uncertain in handling the measures included in the policies (Karjalainen and Siponen, 2011, p. 519). The socio-organisational resource which contains the compliance of information security policies by employees is subject to growing interest in practice and research (Bulgurcu et al., 2010, p. 524).

For the research, theories from different research fields are used to investigate employees' information security behaviour (Bulgurcu et al., 2010, p. 524; Lebek, Uffen, Neumann, Hohler and Breitner, 2013, p. 3). The foundations for this study represent the theory of transformational leadership introduced by Bass (1985) and the social learning theory introduced by Bandura (1977). In prior research, transformational leadership was identified as positively influencing employees' behaviour in order to enhance their performance level beyond expectations (e.g. Cavazotte, Moreno and Bernardo, 2013). Furthermore, assumptions about external cues of the informal social learning environment were confirmed in prior research regarding their positive influence on security behavioural intentions (Warketin et al., 2011). Based on that, the aim of this study is to identify possible factors that can be used to positively influence employees' self-efficacy in order to increase their behavioural intentions towards information security compliance and participation. For this study, as possible factors, the dimensions of transformational leadership and the external cues, present within the informal social learning environment of employees, are used. The informal social learning environment represents the counterpart to the formal learning which entails Security Education, Training and Awareness (SETA) programmes (Warketin et al., 2011, p. 268). In the context of this study, information security behavioural intentions are divided into security compliance and participation intention, adapted from the research field of workplace safety. Security compliance intention describes the observance of only the minimum of information security requirements at the organisation to maintain information security. Security participation intention, however, refers to behaviour that goes beyond meeting the information security requirements (Innes, Turner, Barling and Stride, 2010, p. 279; Clark and Ward, 2006, p. 1176; Neal and Griffin, 2006, p. 947). For the following research question, a research model was developed and empirically analysed:

RQ: *How do transformational leadership and an informal social learning environment influence employees' security behaviour?*

The study is structured as follows: In Chapter 2, the present state of research is shown. Furthermore, the underlying theories (transformational leadership and social learning theory) are represented and the justification for a joint analysis of both theories is given. Chapter 3 entails the research model and hypothesis generation. Following that, the research design is represented in Chapter 4, including the data collection process and the data analysis. In Chapter 5, the results of this study are represented. The results are separated into results from the exploratory factor analysis and results from the structural equation modeling. Afterwards, the results are discussed in Chapter 6. Chapter 7 shows the limitations of this study and in Chapter 8 the conclusion is drawn and an outlook for future research is given.

8. Conclusion and Outlook

The results of this study contribute to the knowledge in the field of employees' information security behaviour. In a first attempt in research, the dimensions of transformational leadership and social learning theory were jointly examined in order to analyse their impact on employees' self-efficacy. Self-efficacy in this regard describes employees' beliefs in their ability to comply with information security policies. By using self-efficacy as a mediating variable, the indirect impact of transformational leadership and social learning theory on security compliance and participation intention were examined. In particular, leadership receives increasing attention in information security context where technical solutions alone are not sufficient. The obligations to ensure information security, imposed by laws and regulations, bring companies to take all measures necessary to enhance employees' information security performance. The human factor bears great risk in this regard. Therefore, it is important to investigate possible influential factors that can enhance employees' compliance behaviour. The study could not prove a relation between the dimensions of transformational leadership and self-efficacy and thus no indirect influence on security compliance and participation intention. The influence of the external cues of the informal social learning environment on self-efficacy was mainly proven. Since the positive influence of self-efficacy on security compliance and participation intention was confirmed, the indirect influence of the external cues on employees' behavioural intentions was confirmed as well. In this respect, several managerial implications were derived in order to enhance employees' security performance. Security Education, Training and Awareness (SETA) programmes represent an important measure to increase employees' awareness of the importance of information security and to train employees' in the execution of the security policies. In addition to trainings, the influential factors, present in the informal social learning environment of employees, can be used. It is advisable that all necessary working resources are available to employees which enable or facilitate the compliance with security policies (situational support). Further, experienced employees can serve as object of observation. Inexperienced employees should get the opportunity to observe their colleagues comply with the security policies in order to learn from them (vicarious experience). Although a positive influence of verbal persuasion on self-efficacy was not confirmed, feedback can be supportive to assess employees' capabilities and to point out the importance of compliant behaviour. Ultimately, the working environment has to be organised so that it can positively influence employees’ self-efficacy to enhance their information security performance.

In future research it could be interesting to examine this study cross-culturally in order to achieve generalisability of results and to compare across different cultural settings. It would also be interesting to analyse the relation between transformational leadership and self-efficacy more deeply which seems to be a very complex relation. Therefore, further interaction effects could be considered. Additional antecedents that influence employees’ self-efficacy could be integrated into the model. In this study, only transformational leadership was analysed. For future research, transactional leadership as exogenous variable should be considered as well. Besides, one could consider further mediating variables that link the relation between the exogenous variables such as leadership and elements within the workplace environment and employees behavioural intentions towards information security. In addition, it would be interesting to think of further elements within the working environment.