Discussion of the Leadership Impact on Mobile Security

Masterarbeit

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

vorgelegt von

Name:	Özhan	Vorname:	Bora
[redacted]	[redacted]	[redacted]	[redacted]

Prüfer: Prof. Dr. Michael H. Breitner

Hannover, den 29. September 2015

Table of Contents

Abstract

Innovations in computing and communication technologies have a transformative effect on the way information is accessed, used and stored today. Thereby, the emerging trend of IT consumerization increases the importance of mobile information security in organizations and represents new challenges for the IT management. Besides technical solutions, research has incorporated multidisciplinary behavioural theories in order to explain employees' mobile information security awareness and behaviour. While emphasizing employees as the weakest link in the information security chain, the role of leadership has been considered less. To address this gap in research, the purpose of this explorative study is to investigate how dimensions of leadership can influence employees' mobile information security behaviour. A research model is developed, integrating the theory of leadership, the protection motivation theory (PMT) and the theory of planned behaviour (TPB). On the basis of expert interviews, the results indicate an indirect influence of leadership on employees' intention to comply with the organizational mobile information security policy (MISP). Further, the findings show that especially employee perceptions of response efficacy, self-efficacy and subjective norms mediate the impact of leadership on MISP compliance intention. The data analysis did not support the negative relationships between employees' threat perceptions and efficacy perceptions. Drawing from study findings, implications for research and practice are discussed.

Keywords: *Mobile information security, employees' security behaviour, leadership, protection motivation theory, theory of planned behaviour, IT consumerization*

1. Introduction

The high level of digital connectivity, powered by innovations in computing and communication technologies, has a transformative effect on the way information is accessed, used and stored (Dinev and Hu, 2007, p. 387). Rapid changes in the form and usability of mobile devices as well as mobile data networking technologies have facilitated new types of global information sharing (Tu and Yuan, 2012, p. 1393). The emerging trend of IT consumerization is defined as an environment that allows employees to mix the private and enterprise use of mobile devices and services (BSI, 2013, p. 7). When used for business purposes, mobile devices can increase convenience, efficiency and productivity of employees. At the same time, they bring new risks to information security since they are fundamentally more vulnerable to threats than stationary computer systems. In this case, the concerned security is referred to as "mobile (information) security" and represents an emerging discipline within information security (Tu and Yuan, 2012, p. 1393). Sensitive corporate information is easily transported outside managed environments, which is why the trend of IT consumerization has dramatically increased the number of expensive security incidents. A recent research in the field of information security, which was conducted by Dimensional Research, confirmed the broad use of mobile devices in almost all organizations. 95% of the interviewed IT professionals affirmed that mobile devices such as smartphones or tablets are allowed to connect to their corporate networks. With the high rate of used mobile devices, it is unsurprising that the number of security incidents is also expected to be high. According to the same survey, 79% of these organizations reported mobile security incidents in the past year (Dimensional Research, 2014, pp. 2).

As these figures demonstrate, threats related to mobile information security are a major challenge for many organizations since these threats may have dire consequences, including corporate liability, loss of credibility, and financial damage (Bulgurcu et al., 2010, p. 524). Hence, the topic of mobile security grows in importance and becomes part of the key priorities of top management (Tu and Yuan, 2012, p. 1393; Dimensional Research, 2014, p. 2). In order to reduce the risk of mobile 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 and Vance, 2010, p. 487; Vroom and von Solms, 2004, p. 193). According to the aforementioned survey, careless employees are a greater security threat than cybercriminals, ignoring compliance with basic security procedures (Dimensional Research, 2014, p. 8). For this reason, literature often refers to employees as the weakest link in the information systems (IS) security chain (Ifinedo, 2012, p. 84). This in turn, reinforces the importance of implementing a strong combination of technology and security awareness throughout a company.

Organizations, especially IT executives and IT professionals, establish mobile information security policies (MISP) that provide employees with guidelines on how to ensure mobile information security while performing their daily work (D’Arcy et al., 2009; Bulgurcu et al., 2010, p. 524). Nevertheless, the lack of employees’ security awareness or the lack of technical knowledge regarding the implementation of measures determined in the MISP can result in non-compliance among the staff (Karjalainen and Siponen, 2011, p. 519). While developing guidelines and policies is an important starting point, it is not enough to ensure employees’ compliance with them. Therefore, an understanding of which determinants motivate employees to comply with their organizations’ MISP is essential for IT executives to diagnose the deficiencies in their mobile information security management efforts (Bulgurcu et al., 2010, p. 524). For this purpose, theories from different research fields are used in the present study. The theories of transactional and transformational leadership, introduced by Bass (1985), the protection motivation theory (PMT) by Burns (1975) and the theory of planned behaviour (TPB), proposed by Ajzen (1991) represent the foundation of this paper. Previous scholars described transformational leadership as positively affecting employees' behaviour in order to enhance their performance level beyond expectations (e.g. Cavazotte et al. 2013). Other studies demonstrated that sanctions like formal control measures, which are associated with transactional leaders, are capable of inducing compliant behaviour by employees (e.g. Siponen and Vance 2010; Hovav and D'Arcy 2012). Furthermore, constructs of the PMT and TPB were confirmed in prior research concerning their positive influence on employees' security behavioural intentions (e.g. Herath and Rao 2009; Bulgurcu et al. 2010; Johnston and Warkentin 2010). Based on that, the aim of this thesis is to identify determinants of the two leadership styles, which (indirectly) influence employees' MISP compliance intention. Thus, the primary research question to be addressed in this study is:

RQ: How does leadership modify employees' behavioural intentions associated with recommended individual mobile device security actions?

The remainder of this paper is structured as follows: After this introduction, the present state of research is shown in chapter 2. Furthermore, the trend of IT consumerization and the emerging discipline of mobile information security are explained. The chapter ends with a presentation of the underlying theories (transactional and transformational leadership, PMT and TPB). Chapter 3 entails the research model and hypothesis generation. Subsequently, the research design and methodology are described, including the qualitative data collection process and data analysis. In Chapter 5, the results of this research are presented. In the following stage, the results and the implications for research and practice are discussed. After a consideration of limitations and an outlook for further research, the paper finally ends with the conclusion.

2. Theoretical Background

2.1. Literature Review

In the beginning, existing literature was searched and reviewed in order to analyse the status quo in the field of research how leadership impacts mobile information se-

8. Conclusion and Outlook

Rapid changes in the form and usability of mobile devices as well as mobile data networking technologies have facilitated new types of global information sharing (Tu and Yuan, 2012, 1393). The emerging trend of IT consumerization is defined as an environment that allows employees to mix the private and enterprise use of mobile devices and services. While mobile devices can increase convenience, efficiency and productivity, they bring new risks to information security as they are fundamentally more vulnerable to threats than stationary computer systems. In this context, technical solutions are not alone sufficient, thus the role of leadership receives increasing attention. Instead of ignoring the risk bearing human factor, it becomes important to examine possible influential factors that can enhance employees' compliance behaviour with organizational policies and procedures. Hence, ensuring mobile information security is part of the key priorities of the top management.

The results of this study contribute to the knowledge in the field of employees' mobile information security behaviour, as it aims to explain the relationship between full range leadership and employees' MISP compliance intention. Previous studies mentioned especially transformational leadership in the context of information security. However, the role of IT managers in the information security chain has received little attention. Thus, the examination of full range leadership was necessary in order to explain employees' intention to meet mobile information security standards. To address this gap, the concept of transactional and transformational leadership was introduced in the field of employees' mobile information security behaviour and jointly examined with the theory of protection motivation and the TPB. By using selected determinants of the PMT and TPB as mediating variables, the indirect impact of leadership as well as the direct influence of PMT and TPB constructs on employees' MISP compliance intention was investigated. In line with the vast literature, which has considered the importance of PMT and TPB constructs in the field of information security, the results of this thesis prove the direct and significant impact of response efficacy, self-efficacy and subjective norms on employees' compliance intention with MISPs. There is one restriction with regard to the perceptions of self-efficacy of non-IT employees. This group seems to be more influenced by fear as the result of awareness and less by the utility of protective technologies and policies. Further, this paper contains potentially important implications concerning the role of leadership in enhancing employees' MISP compliance intention. The results prove that leadership is strongly related to employees' mobile security behaviour. It could be shown that employee perceptions of response efficacy, self-efficacy and subjective norms mediate the influence of leadership on MISP compliance intention. Accordingly, leaders or IT executives possess the ability to (indirectly) enhance employees' intentions. Moreover, the results indicate that managerial communications appealing to users' perceptions of threat severity and vulnerability will enhance their compliance intention with the organizational MISP. Since policies are norms that include imperative forms, there is a need for argumentation and justification to change employees' cognitive states. This kind of persuasive action linked with active participation by serving as a role model should constitute the basic publication of mobile security regulations. In this connection, SETA programmes represent an important measure to increase employees' awareness regarding the importance of mobile information security and to train employees' in the execution of the policies. However, employees vary widely in their level of threat awareness and knowledge of how to control their individual mobile computing capabilities; thus a single approach to this form of communication is not advised. Instead, IT managers must devise a strategy in which end users are exposed to awareness-raising measures with language suitable to their efficacy level and trainings suitable to their technical capabilities. Simultaneously, these measures can serve as an instrument to develop an appropriate group security culture, which is important to ensure that the actions of employees satisfy the sentiment of management. Finally, a combination of socio-organizational and technical measures is emphasized by IT executives in order to guarantee efficient mobile information security. Regarding the style of leadership, the results show that the analyzed IT executives are applying the behavioural dimensions of both, depending on the particular situation. As transformational leadership is an extension of transactional leadership, there is a fluid transition between the behavioural dimensions. Thus, it is not a surprise that managers are combining these styles. Concluding, organizations need to establish a mixed leadership style that perceives mobile information security as a crucial issue and arranges suitable training and awareness programmes. Ultimately, the purpose needs to be the implementation of company rules into the routine behaviour of employees. Obviously, the creation of a security-aware company culture on all corporate levels is therefore the ideal.

Future research could enlarge this study across different cultural settings in order to achieve generalisability of results and to compare these cross-culturally. Moreover, it would be interesting to analyse further mediating variables that link the relation between leadership and employees' MISP compliance intention. Besides, the direct influence of perceived threat vulnerability and perceived threat severity on employees' MISP compliance intention deserves a more detailed consideration in further research. In addition, this study focused on IT executives and managers, who are responsible for IS security in their organizations. In future studies, executives outside the IT department could be integrated into the examination. It would be interesting to analyse the degree of transactional and transformational leadership within different departments. Future research should explore, whether non-IT managers are emphasizing the relevance of mobile security and how these are influencing the security behaviour of their employees.