Exploring Security Processes in Organizations: the Case of Smartphones

Lena Reinfelder, Zinaida Benenson

Friedrich-Alexander-Universität Erlangen-Nürnberg

Abstract

We present results of two exploratory qualitative studies of smartphone security in organizations. The first study provides insights into the process of security development. The second study analyzes the effects of smartphone security measures on the productivity and behavior of end users. We find that smartphones create specific conflicts between security and productivity, because they have different technical characteristics and are used for different purposes than laptops and PCs. Nevertheless, security development processes for smartphones do not differ from other security processes, and the conflicts with productivity cannot be observed by security experts due to lack of structured feedback in organizations. Structured user involvement has a great potential to improve alignment of security processes with specific technologies and decrease negative effects of security measures on productivity. This, in turn, can increase the compliance behavior and consequently the organizational security level.

1 Introduction

The borders between private and business use of smartphones have started to blur with the introduction of BYOD (Bring Your Own Device), COPE (Corporate Owend, Personally Enabled) and other policies that allow personal and business use of a device. Despite the manifold advantages of mobile devices in the business context (Bernik und Markelj, 2012; Jacoby et al., 2007), they also pose novel threats to organizations. Smartphones can provide remote access to a variety of sensitive information, are rarely switched off, face an increased risk of being lost or stolen due to their small size and ubiquitous usage. Additionally, they are equipped with several sensors such as GPS, microphone, camera and motion sensor, which could turn the smartphone into a monitoring device.

Although there exist diverse smartphone security measures such as mobile device management systems, VPN connections, firewalls, intrusion prevention systems and anti-virus (Pan und Fung, 2013; Van Bruggen et al., 2013), smartphone security also depends on employee behavior. Especially, when smartphone security measures are circumvented or not applied appropriately, smartphones pose a risk to organizations.

Veröffentlicht durch die Gesellschaft für Informatik e. V. 2017 in
M. Burghardt, R. Wimmer, C. Wolff, C. Womser-Hacker (Hrsg.):
Mensch und Computer 2017 – Workshopband, 10.–13. September 2017, Regensburg.
Copyright (C) 2017 bei den Autoren. https://doi.org/10.18420/muc2017-ws05-0403

Introduction of smartphones, similarly to any other information system, has the goal of increasing effectiveness and efficiency within an organization (Hevner et al., 2004). However, one has to consider the interaction of this technology with the organization and its environment (Silver et al., 1995) in order to fully understand the consequences of its usage. This also means considering the effects of smartphone security measures. In this paper, we investigate the processes surrounding secure smartphone integration and its consequences for the employees and, ultimately, for the organizations.

In the following, we first introduce background and research questions in Section 2. We then present the results of two explorative qualitative interview studies, the first one considering smartphone security measures from the point of view of organizational security experts (Section 3), and the second one considering smartphone security from the employees' point of view (Section 4). Subsequently, we discuss combined findings from two studies to provide insights into the smartphone security development process (Section 5). Finally, we present directions for future research in Section 6.

2 Background

Organizational smartphone security can be considered as an instance of organizational security. Organizational security is subject to different influences, set by the organization as well as by industry, country and cultural characteristics. Influences by the organization include protection goals and measures. Industry characteristics influence protection goals, e.g., by introducing industry standards such as ISO norms. Country characteristics set a legal frame for data processing, and cultural characteristics influence behavior and interactions of different actors.

Security measures implemented by organizations can be technical and behavioral. Whereas manifold technical approaches are available to secure organizational data on smartphones (Ding et al., 2014; Ghosh et al., 2013; Kodeswaran et al., 2012; Russello et al., 2012), behavioral factors are often neglected (Reinfelder und Weishäupl, 2016). As the security of an organization is dependent on both, technical measures as well as secure behavior of the employees, both factors have to be considered in order to successfully establish security (Pfleeger et al., 2014). Therefore, we ground our investigation of smartphone security on the the Dynamic Security Success Model (DSSM) developed in (Reinfelder und Weishäupl, 2016) that considers both factors in the context of security creation process.

DSSM, depicted in Figure 1, combines the Information Systems Success Model (DeLone und McLean, 1992) and Organizational Learning Theory (Argyris, 1976). The technical security development process (*Security Objectives* and *Security Measures*) leads to the consequences for employees (*Use* and *User Satisfaction*) resulting in an *Individual* as well as an *Organizational Impact*. The two feedback loops aim at applying knowledge generated through feedback from individual and organizational consequences to either changing security measures (*Single-loop learning*), or changing security objectives if adapting the measures is not sufficient (*Double-loop learning*). The arrows within the model represent relationships between the constructs, e.g., Security Objectives determine which Security Measures are implemented by an organization.

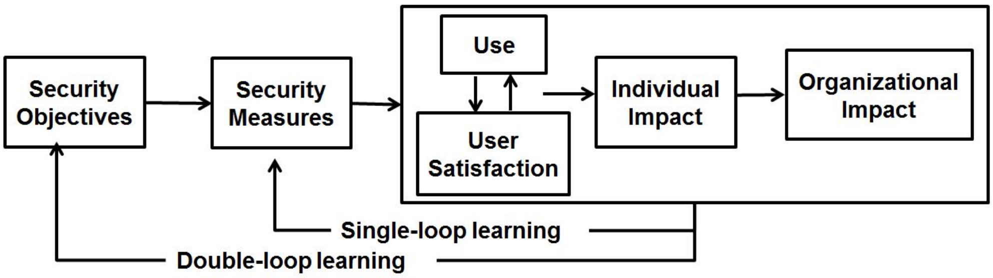

Figure 1: Dynamic Security Success Model (Reinfelder und Weishäupl, 2016)

The literature review of 569 articles conducted in (Reinfelder und Weishäupl, 2016) with respect to the DSSM identified several research gaps which were summarized into eleven research questions to stimulate future research directions. We concentrate our research on the following identified questions:

- What security objectives influence the company's decisions regarding smartphone security?
- How are security measures derived from these security objectives?
- What are the consequences of applied security measures on smartphone use and user satisfaction of employees?

For the first two questions, we interviewed seven IT experts from five large scale German companies (Study 1). For the third question, we interviewed ten employees from different companies (Study 2). In both studies, we used a convenience sampling, asking our acquaintances and colleagues to recommend possible participants to us. In the subsequent sections we present the results of these two studies.

3 Study 1: The Security Development Process

We conducted semi-structured interviews with seven experts working in the IT department of five large scale German companies to gain insights into the security development process for smartphones. An overview of the experts' positions and industry sector can be found in Table 1. We asked the experts to describe how security objectives for smartphones are set and how the decisions on security measures are made.

Interview data were transcribed verbatim, covering 371 minutes of audio material. We used a grounded theory approach for data analysis (Corbin und Strauss, 2015), which was conducted by two independent researchers. Results were generated by annotating and discussing individual statements with the aim to derive categories. Then, case descriptions were created in order to allow a comparative analysis between the different cases.

The process of security development in organizations that emerged from the interviews is shown in Figure 2. Although we specifically asked about smartphones, the experts emphasized that this process is the same for all security measures. Security objectives of a company

Table 1: Industry sector and expert position (the numbers in brackets represent the number of respondents)

Industry	Postion
Technology Group	Security Manager (1)
Healthcare	Security Manager (2)
Telecommunication	Project Security Manager (2)
Consulting	Senior IT Consultant (1)
Semiconductors	Managing director (1)

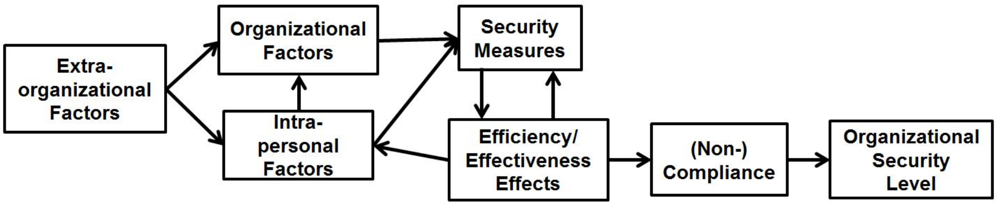
Extra-organizational Factors
Organizational Factors
Intra-personal Factors
Security Measures
Efficiency/ Effectiveness Effects
(Non-) Compliance
Organizational Security Level

Figure 2: Security development process that emerged from the interviews

are subject to different influencing factors. *Organizational Factors* reported by the IT experts are defined by the organizational culture (e.g., the kind of data processed within the company) and structure. This includes economic circumstances, such as available budget, the expected economic benefit as well as the expected loss due to a lack of security.

Although the IT department determines the required actions according to the cultural and structural circumstances, *Extra-organizational Factors* from outside the company influence decisions about security measures. Legal requirements may restrict or specify the framework for implementing security practices, e.g., how data has to be stored and processed. Industry standards (e.g., ISO norms), may serve as guidelines for implementing security and can be used as a qualitative characteristic when then company undergoes a certification process. Technical development of smartphones as well as new attacks and security solutions also influence decisions. All these factors shape processes and set requirements and rules that guide the day to day work of developing and implementing security measures.

Intra-personal Factors describe the views and perceptions of actors within the company regarding extra-organizational and organizational factors. They further include the views and knowledge of the the IT experts about the interaction between the employees and security measures. Intra-personal factors therefore influence organizational factors by affecting and changing organizational processes and structures, and so also influence the development of security measures.

Efficiency/Effectiveness Effects describe the influences of implemented security measures on the daily working tasks of employees regarding their smartphone. IT experts report that security measures have either no obvious implications for the employees, or they may have obvious negative implications on the effectiveness of the tasks, usually by completely preventing a use case (e.g., downloading apps from the official stores is disabled on the smartphone) or on the efficiency of the tasks (e.g., encryption of emails slows communication down). In such cases, security measures result in the negative feedback to the IT department and have to be adapted to maintain the usefulness of smartphones.

Efficiency and effectiveness effects influence security measures through end user feedback. One company reported that in order to integrate smartphones, the IT department tested a Mobile Device Management solution with a focus group. Due to negative usability feedback, the company decided against introducing this solution. Within the remaining companies, feedback is gathered rather sporadically, e.g., by analysing the company's social media for comments on security measures. There is no established procedural approach to how to create, select or analyze the feedback. Regarding the influence of the intra-personal factors, user behavior and requirements are often interpreted based on personal opinions and experiences of the security experts without established evidence. This results in a negative perception of employees as being uninterested in security and weakening it whenever possible.

Besides evoking feedback, efficiency/effectiveness effects further determine whether employees comply with security measures or not. If the employees refrain from complying with security measures, the IT departments often try to enforce compliance by technical means, e.g., by disabling the access to the official app store in order to prevent the employees from using disallowed applications. The *(Non-)Compliance* then results in the overall *Organizational Security Level*, which is the outcome of technical security measures and user behavior.

4 Study 2: Implications of Smartphone Security

To gain the employees' perspective on the smartphone security, we conducted semi-structured interviews with five male and five female employees of various business sectors (Table 2). The data collection process was divided into three main parts. Firstly, the respondents explained their working tasks, including, but not limited to, the role of the smartphones. Secondly, the guidelines and security measures for smartphones were described by the respondent. Finally, the participants were asked about their possibilities to shape the smartphone security measures, either in the development phase or after they have been implemented. The interviews were conducted via telephone and lasted 17 minutes in average. All interviews were transcribed verbatim and analysed using qualitative data analysis (Schreier, 2012). A coding frame, consisting of 15 main and 18 sub categories, was developed and defined by two researchers iteratively. The data was then coded by the two researchers independently (Cohen's Kappa = 0.91). For example, the main category *Preventive security* includes six subcategories: *Access control, Policies, Training, Cyptography, Authentication, Data control*. The main category *Feedback* includes two subcategories: *Form* (e.g., questionnaires) and *Type* (e.g., complaints).

Implications of smartphone security measures are divided into three categories: implications with no constraints, implications with constraints and implications with behavioral change.

Implications with no constraints: Although participants reported that certain functionalities are not available due to security reasons, they did not feel that this had negative implications, as this did not impact their tasks: *"In order to access the internet you need a certain user login*

Table 2: Demographic data of interview participants

Participant	Business Sector	Position	Gender	Age
P1	Automotive suppliers	Production team leader	Male	50
P2	Electrical engineering	Branding manager	Female	35
P3	Electrical engineering	Marketing manager	Female	39
P4	Medical technology	Application manager	Male	28
P5	Medical technology	Project manager	Female	44
P6	Technical engineering	Marketing manager	Female	41
P7	Telecommunication	Employee field service	Male	55
P8	Butcher	Manager	Male	50
P9	IT development	Financial manager	Female	37
P10	Electrical engineering	Manager	Male	45

which you have to apply for. But we don't need the Internet." (P1). P2 mentioned that missing access to the organizational intranet was not disturbing to her.

Implications with constraints: Participants reported that some smartphone security measures were experienced as disturbing, but did not result in a changed behavior, as the respondents did not see any possibilities to circumvent them, e.g.: *"We have to change our password every 90 days in order to access our mails on the smartphone." (P5)*. If P5 forgets to update her password, she cannot receive any new emails on her smartphone, which already has happened before. P4 reported on missing access to the intranet that complicates work, and P3 mentioned faulty updates which are corrected only after some time.

Implications with behavioral change: Smartphone security measures can have implications constraining the work task of the employee leading to a behavioral change. Security measures are then either not used at all (e.g., encryption of emails is removed, as, according to P2, it does not work on smartphones) or an alternative possibility is used. For example, P7 reports: *"We have a policy (...) that we are not allowed to install any apps which are not from the company. I therefore use my private smartphone for useful apps which I also use for my work."* P7 is mainly working while on the move and uses his smartphone to facilitate his work (e.g., finding gas stations). However, the company does not allow to install appropriate apps, which results in P7 using his private smartphone and thus circumventing the company policy. Further respondents described the use of alternative communications tools, e.g., using WhatsApp instead of SMS (P3), or the use of laptops instead of the smartphone, e.g., when encrypted emails cannot be read on the smartphone (P3, P4, P10).

Feedback from employees: We asked our participants if they knew about any form of security evaluation within their company. Five respondents mentioned contacts forms, hotlines and email addresses for feedback. However, they did not know what impact their feedback had on security processes. The remaining respondents were not aware of any feedback possibilities.

5 Discussion

We combine our findings from the presented studies to deepen insights into the smartphone security development process. Considering the reports of the employees, it seems that many security conflicts are related to smartphones crossing perimeter security of the companies in an unexpected way and having different technical characteristics than laptops and PCs. Thus, when smartphones are used on the move, users need to install apps that facilitate travel, which is not allowed for the fear of malicious apps gaining access to internal resources of the company. Within the company, employees need access to the intranet, but smartphones do not have this access, as they seem to be considered as external devices even within company's physical boundaries. Moreover, different password expiration policies are applied to email usage on smartphones versus on other devices, and email encryption works on laptops, but not on smartphones. Coping strategies sometimes result in the usage of shadow IT (Behrens, 2009), where employees use unapproved hardware (e.g., private smartphones) or software (e.g., WhatsApp) to complete their tasks.

While security experts provided us with valuable insights into the structure of security processes in organizations, the actual effects of security measures on employees were not well known. Disturbing influences and behavioral changes due to security measures were difficult to observe for the experts, because the employees were mostly not directly involved in the security process. Therefore, extending the intra-personal factors with structured user involvement would clearly decrease negative effects of security measures, thus increasing the compliance behavior and consequently increasing the organizational security level.

6 Conclusion

We conducted two exploratory qualitative studies on the interplay of technical security means and user behavior in business smartphone use. Empirical findings reveal that user behavior is underrepresented in organizational security development processes thus leading to negative effects on the effectiveness and efficiency of smartphone usage, which may result in non-compliant behavior that weakens organizational security. Due to exploratory nature of the studies, our findings have some limitations: they cannot be generalized, and we did not have access to experts and end users working at the same company, such that we could not compare and contrast their views within the same organization.

Based on our results, we aim at conducting a single case study within one large scale company. We seek to analyze the impact of active employee feedback on the development of security measures with the goal to decrease negative effects of security on smartphone use and thus increase the overall organization's security level.

References

Argyris, C. (1976). Single-loop and Double-loop Models in Research on Decision Making. *Administrative Science Quarterly*, 363–375.

Behrens, S. (2009). Shadow systems: The good, the bad and the ugly. *Communications of the ACM*, *52*(2), 124–129.

Bernik, I. & Markelj, B. (2012). Blended threats to mobile devices on the rise. In *2012 International Conference on Information Society (i-Society)* (S. 59–64). IEEE.

Corbin, J. & Strauss, A. (Hrsg.). (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage Publications.

DeLone, W. H. & McLean, E. R. (1992). Information Systems Success: The Quest for the Dependent Variable. *Information Systems Research*, *3*, 60–95.

Ding, J., Chien, R., Hung, S., Lin, Y., Kuo, C., Hsu, C. & Chung, Y. (2014). A framework of cloud-based virtual phones for secure intelligent information management. *International Journal of Information Management*, *34*(3), 329–335.

Ghosh, A., Gajar, P. K. & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, *4*(4), 62–70.

Hevner, A. R., March, S. T., Park, J. & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, *28*(1), 75–105.

Jacoby, G. A., Ransbottom, J. S., Hickman, T. & Potasznik, M. (2007). Screening Mobile Devices to Examine Network Health. In *40th Annual Hawaii International Conference on-System Sciences (HICSS 2007)* (S. 164–164). IEEE.

Kodeswaran, P., Nandakumar, V., Kapoor, S., Kamaraju, P., Joshi, A. & Mukherjea, S. (2012). Securing enterprise data on smartphones using run time information flow control. In *2012 IEEE 13th International Conference on Mobile Data Management (MDM)* (S. 300–305). IEEE.

Pan, J. & Fung, C. C. (2013). An offensive containment strategy based on Malware's attack patterns. In *International Conference on Machine Learning and Cybernetics (ICMLC)* (S. 1631–1636).

Pfleeger, S. L., Sasse, M. A. & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), 489–510.

Reinfelder, L. & Weishäupl, E. (2016). A Literature Review on Smartphone Security in Organizations using a new theoretical Model-The Dynamic Security Success Model. In *Proceedings of the Pacific Asia Conference on Information Systems (PACIS) June 27–July 01, 2016, Chiayi, Taiwan*.

Russello, G., Conti, M., Crispo, B. & Fernandes, E. (2012). MOSES: supporting operation modes on smartphones. In *Proceedings of the 17th ACM symposium on Access Control Models and Technologies* (S. 3–12). ACM.

Schreier, M. (Hrsg.). (2012). *Qualitative content analysis in practice*. Sage Publications.

Silver, M. S., Markus, M. L. & Beath, C. M. (1995). The information technology interaction model: A foundation for the MBA core course. *MIS quarterly*, 361–390.

Van Bruggen, D., Liu, S., Kajter, M., Striegel, A., Crowell, C. R. & D'Arcy, J. (2013). Modifying smartphone user locking behavior. In *Proceedings of the Ninth Symposium on Usable Privacy and Security)* (S. 10).