User Acceptance Identification of Restrictions Caused by Mobile Security Countermeasures

Basel Hasan, Tariq Mahmoud, Jorge Marx Gómez
Department of Computing Science
Oldenburg University
Oldenburg, Germany
{basel.hasan, tariq.mahmoud, jorge.marx.gomez}@uni-oldenburg.de

Reshmi Pramod
Virtual Global University, Frankfurt
Frankfurt, Germany
reshmi.pramod@gmail.com

Joachim Kurzhöfer
Lufthansa Industry Solutions
Norderstedt, Germany
joachim.kurzhoefer@lhind.dlh.de

***Abstract*—The proliferation of mobile devices, especially smartphones and tablets, in people's daily life has motivated the enterprises to embrace mobility as an inevitable success factor in their business. However, integrating mobile devices into enterprises brings new security risks and challenges. Hence, security countermeasures must be applied to mobile devices to secure corporate data and segregate them from private data. Such countermeasures can restrict the usage of mobile devices, and mobile users consequently have to accept the restrictions arising by applying such countermeasures. The user acceptance of these restrictions must be considered. This work derives a set of such restrictions that limit the usage of mobile devices. It also presents the results of a questionnaire that investigates the user acceptance rate of these restrictions. The results of this study might help enterprises in their decision-making process about selecting proper security countermeasures by keeping a considerable balance between security and usability.**

Keywords-mobile enterprise applications; mobile devices; mobile security; user acceptance.

I. INTRODUCTION AND LITERATURE REVIEW

Over the past few years, the evolution of mobile technologies and applications makes the ubiquitous communications (anywhere and anytime) a growing reality [1][2]. According to [3], mobile broadband connections are forecasted to continue growing worldwide to 5.3 billion in 2018, moreover, mobile users will steadily increase to reach 1.37 billion in 2017. In this paper, the mobile user refers to the employee who uses mobile devices (just smartphones and tablets) at work.

The rapid proliferation of mobile devices in people's daily life has triggered enterprises to consider the mobility as an inevitable part of their business and IT strategies to derive more revenue, enhance customer engagements, and being more competitive in the market. Smartphones and tablets became more integrated into enterprises' IT infrastructure. This integration solely represents the enterprise mobility concept by giving the employees better possibilities to work effectively while they are on move [4]. The reasons for this include location flexibility, time saving, portability, ease of research, etc. For example, sale persons can access their mobile Customer Relationship Management System (mobile CRM) to allow them updating their customer details while they are away from their offices.

Many companies provide corporate mobile devices to be used by their employees. Such devices can often be monitored and controlled. On the other hand, the employees can use their own personal devices for work. This concept is considered as a consumerization of IT or Bring Your Own Device (BYOD) [5][6]. In this sense, using corporate or personal mobile devices increases employee productivity and reduces business operational costs [7].

However, companies that allow using mobile devices for work have to pay more attention to the huge amount of new risks that differ clearly from Personal Computer (PC) risks. Smartphones and tablets are lightweight mobile devices. They have low technical capabilities in comparison to PC devices. This hiders these mobile devices from porting PC security technologies and standards [8][9]. Furthermore, mobile devices are small and portable and therefore, they can easily be stolen or lost.

Because of many different risks and risk sources in mobile environments [10]-[13], companies have to apply proper mobile security countermeasures to mitigate such risks. Applying security countermeasures on mobile devices may restrict their usage in a way that affects the mobile users' flexibility and productivity. This in turn influences the decision to use these mobile devices at work. Moreover, this can lead to lose the benefits of mobility. Therefore, companies have to consider such consequences on mobile users when applying new security solutions. One of the biggest barriers to reach a true mobile security is the user acceptance of corporate security policies. As enterprises move to mobile devices, their IT organizations are trying to keep the right balance between user enablement and data security [14].

In this paper, the current mobile security countermeasures are defined based on literature and best practices, and the user acceptance of the accompanying restrictions is investigated quantitatively (see Section IV). The work contributes to the security in mobile applications' research domain in the definition of user acceptance, creation a catalogue/list of the investigated restrictions (consequences) and then ana-

 ISBN: 978-1-61208-417-6

lyzing them by investigating the relationships between these restrictions and the acceptance rate of the enterprises' users. These contributions might be of a great assist for enterprises in their decision-making process, especially when they select security countermeasures by keeping a considerable balance between security and usability.

This paper focusses on the user acceptance rate of mobile security countermeasures in business sectors, where the employees are allowed to use mobile devices for working purposes. The rest of this paper is organized as follows: Section II presents the related work. Then, Section III presents a list of security countermeasures along with their possible accompanying restrictions on mobile users. Section IV presents the results of a conducted questionnaire that measures the user acceptance rate of potential restrictions. Finally, the paper sums up with a conclusion in Section V.

II. Related Work

In order to investigate the user acceptance of new technologies, the Technology Acceptance Model (TAM) has been often conducted [15]-[17]. This model addresses why users accept or reject information systems and how the user acceptance can be affected by system design features [18]. User technology acceptance broadly refers to an individual's psychological state with regard to her or his voluntary and intentional use of a technology. It has been also identified as fundamental challenges to organizational technology adoption [15]. In [16], an extended TAM for mobile government systems has been proposed. However, in that work, the security was not taken as a factor that affects users' decisions to accept using mobile systems.

Another work that is located in this topic has investigated the user acceptance of a Privacy-Enhancing Technology (PET) that is called "Attribute-Based Credentials", or Privacy-ABCs [17]. This work considered the security and privacy as factors that affects the user acceptance of the PET without considering mobility.

In [19], a framework to design secure Mobile Enterprise Applications (MEAs) has been presented. That framework mainly supports the enterprises in decision-making process during designing secure MEAs, side by side in keeping a balance between mobile security and user acceptance. It is stated in that work that the companies have to check user acceptance of security countermeasures even in the design phase of adopting mobile applications. This can be determined through a questionnaire, in which, employees of the enterprise can respond about the potential restrictions.

These related works motivate the objective of this study in investigating the user acceptance rate on the restrictions that accompany the security countermeasures the enterprises enforce while allowing their users to use their mobile devices at work. This paper does not introduce a TAM extension. Rather it investigates the business user's acceptance of the restrictions that are caused by the applying security countermeasures on mobile devices. Such investigation has not been conducted in the related work in this domain so far.

III. Mobile Security Countermeasures and their Accompanying Restrictions

Enterprises need to implement suitable security countermeasures to mitigate the wide range of threats in the mobile environment and achieve a certain level of security on mobile devices. Applying security countermeasures to mobile devices can restrict the usability of those devices. In general, a high level of security on mobile devices can be achieved by setting a high level of restrictions, but on the other hand, this will reduce their usability. These restrictions negatively affect the satisfaction factors of the employees who want to use mobile devices in business sectors. Therefore, enterprises have to balance between the technical view (security solution) and the user view (user acceptance of the restrictions). Hence, a balance between security and usability have to be maintained [20]. The rest of this section goes through a number of mobile security countermeasures collected from literature and best practices. Furthermore, these countermeasures are classified in groups along with their potential restrictions.

A. Authentication and Authorization

Authentication involves identifying the mobile user who needs to have access on certain corporate data. This is usually based on one or a combination of the following types of credentials: something you have (certificate), something you are (fingerprint), something you know (password). In [21], a number of authentication methods for mobile devices has been presented and classified in groups (knowledge-based methods like passwords, Personal Identification Numbers (PIN) or pattern locks as well as biometrics methods like face recognition and voice recognition). In order to control the access to corporate resources, the authenticated mobile users should be also authorized through authorization process, which grants or denies specific permissions to each user.

In addition, mobile devices can be authenticated through continuous touch-based authentication, which continuously records touch data from mobile device's touch screen and then exploits user interaction data to authenticate users based on the way they perform touch operations [22][23]. However, this mechanism is not included in the conducted survey, because it is not widely known in the practice so far.

Consequences on Mobile Users. Strong authentication requires a strong password, which enhances the security on mobile devices. High restrictions can be applied on mobile devices by enforcing long alphanumeric passwords that will be required frequently and might lock the user after few wrong attempts. Such high restrictions enhance the security, but on the other hand, minimize the usability and reduce employees' productivity.

B. Encryption

Virtual Private Network (VPN) is one alternative to enable secure connection between an enterprise's internal network and mobile applications by installing a VPN client on mobile devices [24]. VPN is an alternative to secure sensitive business data "in motion" over unsecured network. In addition, to countermeasure the possible disclosure of sensitive

 ISBN: 978-1-61208-417-6

data that stored on mobile devices (data-at-rest), mobile device's local storage has to be encrypted. Strong encryption mechanisms are used to protect the confidentiality and integrity of communications. By using these encryption and mutual authentication mechanisms, the risk from using unsecured mobile networks before transmitting any data can be mitigated [25].

Many mobile users use personal mobile applications (e.g., Dropbox, iCloud) to centrally store documents in cloud and synchronize them with their multiple computing endpoints. Such mobile applications can take corporate documents out of IT control if those documents are moved to such personal clouds. Therefore, mobility also needs data encryption while they are "in use", which includes maintaining encryption of whatever is being viewed in the file system while being used by a mobile application as well as data shared via Open In or Copy-Paste to another mobile application on the mobile device (i.e., opening an email attachment into a document editor) [14].

Consequences on Mobile Users. Excluding the slower performance that might be caused, no major consequences on mobile device usage have been found when applying encryption on data-at-rest and data-in-motion. In general, enabling security features affects the performance, regarding time and computational power to execute cryptographic algorithms, and users have to find a compromise while choosing ease of use and performance versus security [26].

Concerning data-in-use encryption, the mobile device's performance will be even slower than the case of encrypting data-at-rest and data-on-motion, due to full memory encryption. Anyway, if the data-in-use encryption is not implemented, the company may disallow their employees from using cloud services. This restricts the usage of third mobile applications on mobile devices. Otherwise, the company should have control on Open In and Copy-Paste functions [14].

C. Mobile Physical Security

Lost and stolen mobile devices are seen as the greatest security concern, due to the risk of compromising their data. Hence, mobile device's physical security should be given higher importance. When mobile devices are lost or stolen, the enterprises should not lose control on those devices. Such control can be done using Mobile Device Management (MDM) systems, which enables IT departments to remotely lock and reset mobile devices and wipe their data [27]. Furthermore, to mitigate the risk of compromising the data of lost or stolen mobile devices, a layered mitigation strategy can be conducted [25]. The first layer involves a required authentication before gaining access to the mobile device or corporate resource. The second layer involves either encrypting the mobile device's local storage, or not storing data on mobile devices at all (read only). The third layer involves mobile user training and awareness, which can reduce the frequency of risks related to mobile device's physical security.

Consequences on Mobile Users. Controlling mobile devices by remotely locking and resting has no consequences that can restrict the mobile devices' usage. However, if the layered mitigation strategy is conducted, restrictions can be set in the first layer during authentication (see Section III-A). In the second layer, the user can experience slow performance if the mobile device's local storage is encrypted (see Section III-B). Furthermore, a high level of mobile's physical security may require that no data will be allowed to be locally stored on mobile devices. Consequently, the user will not be able to access corporate documents offline on the mobile device. The third layer concerning the mobile user training will be presented in Section III-F.

D. Protection against Untrusted Applications.

The simplest way to protect mobile devices against untrusted third party applications is to enforce a policy that prohibits the installation of all third party applications. However, this way restricts the mobile device's usage and the mobile user's acceptance rate of such restrictions will be low (see Section IV-C). The alternative is the implementation of whitelisting to prohibit installation of all unapproved third party application. MDM systems utilize the whitelisting for allowing or blocking applications running on mobile devices [28]. Some enterprises implement a sandbox that isolates the corporate date and applications from third party applications on the mobile device. An application runs in a sandbox has file areas, which can only be accessed by the application itself [29].

Consequences on Mobile Users. The mobile user will not be able to install third party mobile applications on the mobile device if the enterprise applies a policy that prohibits the installation of all third party applications. Regarding the second alternative, if whitelisting is applied, the user will still be able to install third party mobile applications, which are approved and included in the whitelist. Finally, if a sandbox is implemented, the user should be able to install third party mobile applications.

E. Firewalls and Antivirus Protection.

To prevent data leakage via malware that is already installed on mobile devices, firewalls are also implemented on mobile devices to block or audit disallowed connections to or from mobile devices [30]. In the traditional desktops, firewalls can restrict access to system services and prevent applications on the system from leaking sensitive information to third parties. Regarding mobile devices, the firewalls can also restrict the network access to data-sensitive applications when not using Wi-Fi network. This is because network connections using mobile 3G/4G networks are usually either expensive or volume restricted [31]. Other way of protection is using antivirus software that can be installed on mobile device to detect malware.

Consequences on Mobile Users. Firewalls and antiviruses software protection can slow down the entire mobile system because these software's functions are always running in the background. The battery consumption can also be a big concern. The enterprises must have control on firewalls and antivirus software to keep them always enabled. However, an enforced firewall policy can affect the mobile users' satisfaction. The system slowness and high battery consumption

 ISBN: 978-1-61208-417-6

are factors that make the employees avoid using mobile devices for work.

F. Conducting Security Awareness

Applying technical security countermeasures to mitigate risks can be insufficient as long as employees are not aware of potential security risks [32][33]. Furthermore, awareness of security risks can improve security countermeasures development (design and implementation) and performance (reduced deficiencies and greater efficiency) [34]. Hence, enterprises have to organize security awareness programs for their employees who want to use mobile devices at work.

Consequences on Mobile Users. Concerning mobile security awareness programs, which are complementary to the technical security solutions, no restrictions on mobile devices' usage has been found so far.

IV. METHODOLOGY

This part describes the research data, the measurement and the methods utilized in the data analysis process. In order to achieve the research objectives and to conduct that in a structured way, few research methodologies have been carried out in this research process. The focus of this study is mainly finding out the various mobile security countermeasures and their restrictions on the enterprises' users who use their corporate mobile devices. This is besides finding out the user acceptance level of these restrictions. For that, a quantitative approach is followed to describe and understand experiences, ideas, beliefs and values. Quantitative research concerns asking people about their opinions in a structured way so that facts and statistics can be produced to guide a study like the one presented in this paper. Briefly, this study analyzes the user acceptance level through observations in numerical representations and statistical analysis.

A. Measurement

For a quantitative measurement, an online questionnaire had been developed to study the perception of users' acceptance rate on the security countermeasures applied on their corporate mobile devices. The pros and cons as well as the reliability of this instrument were also part of the research objectives. The questions were prepared from the information collected from the available literature and best practices in this domain.

The circulated questionnaire had been divided into three main parts and consisted of 17 questions in total. The initial four questions were targeting the mobile device usage at work. The following list of questions targeted the mobile security awareness of users while using their mobile devices. The remaining set of questions were focusing on measuring the user acceptance level of the security countermeasures and their accompanying potential restrictions maintained by the organizations (to protect their data) and applied to the users' mobile devices.

The questions were distributed to the respondents in form of multiple choices questions (using Likert scale items). Users were given the flexibility to choose more than one answer, and they were given space to add their own options.

B. Data Collection

This process focused on collecting the data through distributing the designed questionnaire on a set of targeted respondents who are using their mobile devices at work. The research objectives were achieved from the suggestions of users by targeting corporate areas. According to [35], it is well noted in the literature that managers would ultimately affect firms' practices. Therefore, middle and top managers from information and communication technology domain were considered in this study as main targeted respondents. The questionnaire was circulated in corporate offices and social networking websites. The respondents were given 10 days to complete the questionnaire.

Concerning the sample size, 130 potential respondents were targeted regardless of their age group. According to [36], sample sizes that are greater than 30 and less than 500 are appropriate for most researches and based on that, the selected sample size in this research is considered appropriate. All responses were checked for validity. The incomplete responses were considered invalid and had been excluded. The response rate was 79%. That makes 103 users who provided valid responses. Finally, the data were analyzed using Statistical Package for the Social Sciences (SPSS) statistics software package. Data analysis is explained in the following section.

C. Data Analysis and User Acceptance Rate

The responses to the provided questions had resulted in the following:

- The initial questions were related to mobile devices' usage at work. Around 30% of the respondents stated in this regard that they are allowed to use their mobile devices (own or corporate mobile devices) at work. Only 13% of the respondents were allowed to use only corporate mobile devices.
- Regarding the usage degree of mobile devices for various purposes, the respondents were able to use their devices for corporate purposes considering security as a major concern. The majority of the responses, who were allowed to use mobile devices at work, stated that they were using their mobile devices to access corporate emails (91%), performing work related tasks (52%), access corporate content (70%) and searching for information (69%). Each of these percentages was directly related to a response to a question in the questionnaire.
- When asked about security awareness of their mobile devices, 35% of the respondents had indicated that they have medium to no knowledge about mobile security concerns. This shows that security awareness, training and education were also very important in organizations to protect their data.
- As for dealing with their corporate data, 52% of the respondents answered that they never dealt with their enterprises' data on their mobile devices. Moreover, 30% of the respondents answered that they only dealt with non-

 ISBN: 978-1-61208-417-6

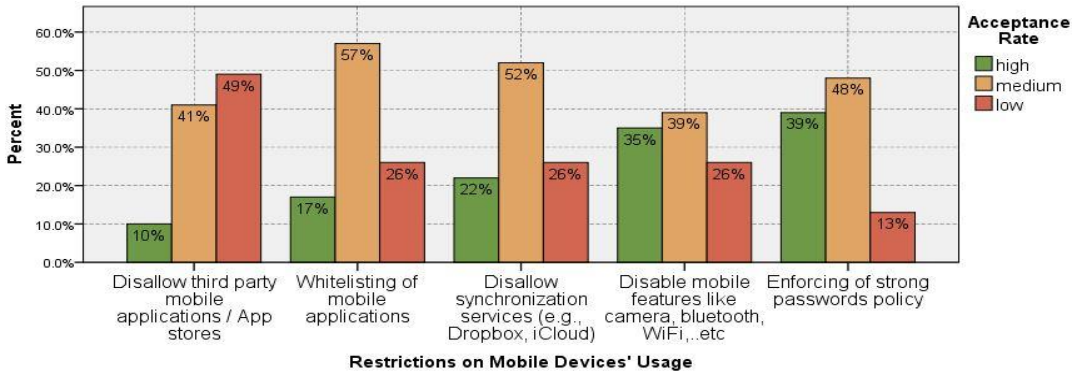

Figure 1. User Acceptance Rate of Restrictions on Mobile Devices' Usage

sensitive corporate data. This comes from several security restrictions applied to these data. An employee, who has to access sensitive corporate data (e.g., sales data, Human Resources (HR) data or policies) using mobile devices, might accept a wide range of restrictions. On the other hand, these restrictions might be not accepted by an employee, who deals only with non-sensitive corporate information.

- Regarding security countermeasures, the majority of respondents, who were allowed to use mobile devices at work, were enforced to apply countermeasures on their corporate mobile devices. The restrictions that arose from applying the aforementioned countermeasures vary from enforcing strong passwords to restricting installation and usage of third party applications reaching the enforcement of full memory encryption. This latter can result in a lower performance of mobile devices.

  The user acceptance rate was analyzed and an excerpt of the restrictions are depicted in Figure 1.
- After listing most of the restrictions the mobile users faced when using mobile devices at work, the last part of the questionnaire investigated whether the users are comfortable with these restrictions or not. Concerning flexibility and productivity, the results (see Figure 2) showed that around 43% of the respondents were not satisfied with the current security restrictions in their mobile working environments.

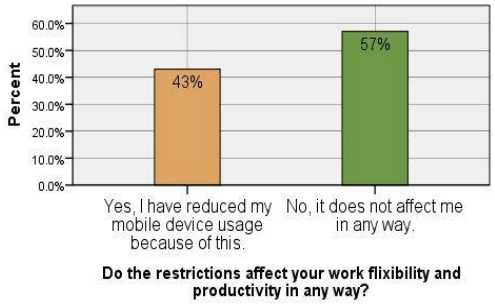

Figure 2. The Effect of Restrictions on Mobile Devices' Usage

D. Recommendations

The mobile user acceptance of the restrictions is a very important factor to be considered during the design phase of MEAs. Evidently, using a strong technical solution must not be on the costs of user's satisfaction. Rather, they have to be considered side by side.

As the enterprises data are usually classified into security levels, enterprises should carefully define the intended security level of their data on mobile devises. The security level should be defined to include three points of view, namely, business view, user view, technical view as depicted in Figure 3. These views are explained as follows: *Business View.* The enterprise defines the security requirements as a subset of its business requirements. *Technical View.* The security requirements are fulfilled by applying the security countermeasures. Implementing the technical solution is accompanied with potential restrictions. *User View.* The user acceptance of the restrictions should be considered as highly important when defining a security level. For instance, there are two alternatives to countermeasure the potential threats that can be caused by third party applications. The first alternative is to disallow the installation of all third party applications on mobile devices. The second alternative is to apply whitelisting. Figure 1 clearly showed that the user accepts the second alternative (whitelisting) more than the first one. This gives enterprises an indicator that the users will be more satisfied with applying whitelisting rather than preventing the installation of all third party mobile applications. In addition, the mobile security countermeasures and restrictions must be taken in such a way that it should not restrict the flexibility and productivity of users. A balance between mit-

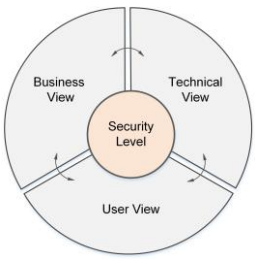

Figure 3. Security Level on Mobile Devices

igating corporate risks and user acceptance has to be taken into account as well. In addition, security awareness programs for employees is a complementary factor for mitigating risks in the mobile environments.

V. CONCLUSION AND OUTLOOK

In this paper, mobile security countermeasures has been derived along with their restrictions on mobile devices' usage. Generally, from a technical point of view, a high security level on mobile devices can be achieved by setting a high level of restrictions. However, this decreases the mobile user satisfactions. A questionnaire has also been conducted to investigate the mobile user' acceptance of the potential restrictions. The user acceptance rate can affect the user decision to use mobile devices. If the user acceptance is low, the user will not be able to use the mobile device at work. Consequently, the company will lose the advantages gained from employing mobility. Having a general overview on the user acceptance rate will help the enterprises in selecting the needed security countermeasures side by side with keeping a balance between security and usability.

In this paper, the extension of TAM was out of the scope. However, the results presented in this paper was part of an ongoing research that will proceed to extend the TAM. This extension will include the applied mobile security countermeasures and their consequences as factors that can affect the user acceptance of using mobile business applications.

ACKNOWLEDGMENT

We gratefully acknowledge that this work is supported by fund coming from Lufthansa Industry Solutions.

REFERENCES

[1] R. Basole and W. Rouse, "Mobile Enterprise Readiness and Transformation," Idea Group Inc. IGI, 2006.

[2] A. Jain and D. Shanbhag, "Addressing Security and Privacy Risks in Mobile Applications," IT Professional, vol. 14, no. 5, 2012, pp. 28-33.

[3] Internet Society, Global Internet Report 2014. Available: http://www.internetsociety.org/sites/default/files/Global_Internet_Report_2014_0.pdf [retrieved: May, 2015].

[4] J. Ranjan and V. Bhatnagar, "A holistic framework for mCRM – data mining perspective," Information Management & Computer Security, vol. 17, no. 2, 2009, pp. 151-165.

[5] D. Sangroha and V. Gupta, "Exploring Security Theory Approach in BYOD Environment," in Smart Innovation, Systems and Technologies, Advanced Computing, Networking and Informatics- Volume 2, M. Kumar Kundu, D. P. Mohapatra, A. Konar, and A. Chakraborty, Eds, Cham: Springer International Publishing, 2014, pp. 259-266.

[6] F. P. Seth, O. Taipale, and K. Smolander, "Role of Software Product Customer in the Bring Your Own Device (BYOD) Trend: Empirical Observations on Software Quality Construction," in Lecture Notes in Computer Science, Product-Focused Software Process Improvement, A. Jedlitschka, P. Kuvaja, M. Kuhrmann, T. Männistö, J. Münch, and M. Raatikainen, Eds, Cham: Springer International Publishing, 2014, pp. 194-208.

[7] H. Hurley, E. Lai, and L. Piquet, Enterprise Mobility Guide 2011. Dublin CA: Sybase, 2011.

[8] J. H. Park, K. J. Yi, and Y. Jeong, "An enhanced smartphone security model based on information security management system (ISMS)," Electron Commer Res, vol. 14, no. 3, 2014, pp. 321-348.

[9] T. Wright and C. Poellabauer, "Improved Mobile Device Security through Privacy Risk Assessment and Visualization," in Data Engineering Workshops (ICDEW), IEEE 28th International Conference on, 2012, pp. 255-258.

[10] W. Jeon, J. Kim, Y. Lee, and D. Won, "A Practical Analysis of Smartphone Security," Human Interface and the Management of Information. Interacting with Information, pp. 311-320, 2011.

[11] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices," in Security and Privacy (SP), 2011 IEEE Symposium on: IEEE, 2011, pp. 96–111.

[12] M. Landman, "Managing smart phone security risks," in Information Security Curriculum Development Conference: ACM, 2010, pp. 145-155.

[13] J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments," in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications: ACM, 2010, pp. 43 - 48.

[14] Good Technology Corporation, Don't Believe the Hype – All Containers are not Equal Protecting the 3 Cs of Se-cure Mobility. [White Paper]. Available: http://media.www1.good.com/documents/wp-dont-believe-the-hype.pdf [retrieved: May, 2015]

[15] C. Lin, P. J. Hu, and H. Chen, "Technology Implementation Management in Law Enforcement COPLINK System Usability and User Acceptance Evaluations," Social Science Computer Review, vol. 22, no. 1, 2004, pp. 24–36.

[16] N. B. Osman, "Extending the Technology Acceptance Model for Mobile Government Systems," development, vol. 5, p. 16.

[17] Z. Benenson, A. Girard, I. Krontiris, V. Liagkou, K. Rannenberg, and Y. Stamatiou, "User Acceptance of Privacy-ABCs: An Exploratory Study," in Lecture Notes in Computer Science, Human Aspects of Information Security, Privacy, and Trust, T. Tryfonas and I. Askoxylakis, Eds.: Springer International Pub-lishing, 2014, pp. 375–386.

[18] F. D. Davis, "User acceptance of information technology: system characteristics, user perceptions and behavioral impacts," International Journal of Man-Machine Studies, vol. 38, no. 3, 1993, pp. 475-487.

[19] B. Hasan, V. Dmitriyev, J. Marx Gomez, and J. Kurzhoefer, "A framework along with guidelines for designing secure mobile enterprise applications," in Security Technology (ICCST), 2014 International Carnahan Conference on: IEEE, 2014, pp. 1-6.

[20] N. Daswani, C. Kern, and A. Kesavan, Foundations of security: What every programmer needs to know: Apress, 2007.

[21] M. Rogowski, K. Saeed, M. Rybnik, M. Tabedzki, and M. Adamski, "User Authentication for Mobile Devices," in Lecture Notes in Computer Science, Computer Information Systems and Industrial Management, D. Hutchison et al., Eds, Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 47-58.

[22] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," IEEE Trans.Inform.Forensic Secur, vol. 8, no. 1, 2013, pp. 136-148.

[23] Z. Cai, C. Shen, M. Wang, Y. Song, and J. Wang, "Mobile Authentication through Touch-Behavior Features," in Lecture Notes in Computer Science, Biometric Recognition, D. Hutchison et al., Eds, Cham: Springer International Publishing, 2013, pp. 386-393.

 ISBN: 978-1-61208-417-6

[24] IBM, IBM Worklight – Mobile Security Measures. Available: http://www-01.ibm.com/software/mobile-solutions/worklight/features/security/ [retrieved: May, 2015].

[25] M. Souppaya and S. Karen, Guidelines for Managing the Security of Mobile Devices in the Enterprise. Available: http://dx.doi.org/10.6028/NIST.SP.800-124r1 [retrieved: May, 2015].

[26] S. Aissi, N. Dabbous, and A. Prasad, Security for mobile networks and platforms. Norwood, MA: Artech House, 2006.

[27] N. Leavitt, "Today's Mobile Security Requires a New Approach," Computer, vol. 46, no. 11, 2013, pp. 16-19.

[28] J. Lee, Y. Lee, and S.-C. Kim, "A White-List Based Security Architecture (WLSA) for the Safe Mobile Office in the BYOD Era," in Lecture Notes in Computer Science, Grid and Pervasive Computing, D. Hutchison et al., Eds, Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 860-865.

[29] H. Orman, "Did You Want Privacy With That?: Personal Data Protection in Mobile Devices," Internet Computing, IEEE, vol. 17, no. 3, 2013, pp. 83-86.

[30] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer, "Google Android: A Comprehensive Security Assessment," Security & Privacy, IEEE, vol. 8, no. 2, 2010, pp. 35-44.

[31] B. Adolphi and H. Langweg, "Security Add-Ons for Mobile Platforms," in Lecture Notes in Computer Science, Secure IT Systems, D. Hutchison et al., Eds, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 17-30.

[32] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, "Employees' Information Security Awareness and Behavior: A Literature Review," in System Sciences (HICSS), 2013 46th Hawaii International Conference on, 2013, pp. 2978-2987.

[33] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Roles of information security awareness and perceived fairness in information security policy compliance," AMCIS 2009 Proceedings, 2009.

[34] J. L. Spears and H. Barki, "User participation in information systems security risk management," MIS Quarterly, vol. 34, no. 3, 2010, pp. 503–522.

[35] F. Duarte, "Working with Corporate Social Responsibility in Brazilian Companies: The Role of Managers' Values in the Maintenance of CSR Cultures," J Bus Ethics, vol. 96, no. 3, 2010, pp. 355-368.

[36] J. T. Roscoe, Fundamental research statistics for the behavioral sciences. Holt, Rinehart and Winston New York. 1969.

 ISBN: 978-1-61208-417-6