# A LITERATURE REVIEW ON SMARTPHONE SECURITY IN ORGANIZATIONS USING A NEW THEORETICAL MODEL – THE DYNAMIC SECURITY SUCCESS MODEL

Lena Reinfelder, Department of Computer Science, Friedrich-Alexander University Erlangen-Nürnberg, Erlangen, Germany, lena.reinfelder@fau.de

Eva Weishäupl, University of Regensburg, Regensburg, Germany, eva.weishaeupl@wiwi.uni-regensburg.de

## Abstract

*Smartphones have become an important part of organizational IT infrastructures including benefits such as increased productivity as well as IT security risks. These risks are mainly related to unauthorized access to corporate data. Integrating smartphones in organizations regarding security involves a sequence of decisions, ranging from the integration approach (smartphones owned by employees or by the organization) to specific security measures implemented on the devices. This is an ongoing process making constant adaption necessary due to progressive development of hard- and software and due to new security risks arising. We propose the Dynamic Security Success Model (DSSM) – a combination of the DeLone & McLean Information Systems Success Model and Argyris' Organizational Learning Theory. This theoretical foundation combines the individual and the organizational impact of smartphone security measures with the learning perspective, allowing a company to respond to the ever changing security requirements of smartphones in organizations. Based on the DSSM, existing literature is reviewed and research gaps are derived for future work.*

*Keywords: Smartphone, IT-Security, Information System Success Model, Organizational Learning, Literature Review.*

# 1 INTRODUCTION

Mobile devices such as smartphones have found their way into our private lives. They facilitate communication, orientation and most important provide mobile access to the Internet. Using smartphones in a business context seems to be a logical consequence.
Smartphones, especially privately owned, are used in all kind of organizations, independent of the company. This integration of smartphones however, implies several security risks for organizational data, such as data leakage by sharing data in the cloud (Gartner 2013). Smartphones are an interesting attack vector due to the huge amount and quality of personal and business data they store, their internal sensors and because they accompany us in daily life (Mylonas et al. 2011).
There exist different approaches to integrate smartphones in organizations, of which one can think of as a continuum with employee handled devices on the one end and corporate handled devices on the other end. This image illustrates that smartphone integration can also be realized by a combination of employee and corporate responsibilities. Smartphone usage in companies is often realized by "Bring Your Own Device" policies, enabling employees to use their private smartphone also for business purposes. However, there are several hybrid forms, for example devices which are bought by the company but configured and maintained by the employee. Another example is smartphones acquired by employees but with corporate software to enable two separate accounts on the device. It is this diversity that hampers a secure integration of smartphones in organizations. Using smartphones in organizations includes the traditional characteristics of a mobile phone – making phone calls, saving contacts and writing short messages. But it includes further functionalities such as accessing the internet, corporate data and sharing these data. We consider the integration of smartphones from a security perspective.
Previous research on smartphone integration into organizations has covered a broad field of topics, often related to the benefits and risks of smartphones in a business context as well as different security solutions (e.g., Mobile Device Management). However, the field of smartphone security is continuously changing. Thus organizations have to adapt to these changes dynamically and learn from previous experiences, especially regarding individual behavior. Therefore, an understanding of smartphone security measures and their effects on the individuals and on the organization is needed. To the best of our knowledge, there does not exist any theoretical model dealing with this dynamical process. We contribute to the IS research area by presenting a new theoretical understanding of smartphone security measures and their impact on an individual and on an organizational level, as well as by presenting a literature review. The underlying research questions are: What are the effects of smartphone security measures on employees and on the organization developed in IS literature? How can organizations learn from experiences with smartphone security measures?
The theoretical foundation is based on the Organizational Learning Theory (OLT) (Argyris 1976) and the Information Systems Success Model (ISSM) (DeLone & McLean 1992), being well established theory and model respectively. The OLT contributes the dynamic of responding to an unintended result of security measures affecting the company in the form of learning. This learning component is based on feedback and enables the company to adapt to IT security risks especially regarding smartphones. The ISSM contributes to our theoretical foundation by including the individual impact into the organizational context, which is of great importance as the security of a company is highly dependent on the behavior of the employees. We present this theoretical foundation – the Dynamic Security Success Model - and provide a structured literature review based on this model including research gaps and research questions for future work.
The paper is organized as follows: Section 2 focuses on the theoretical background, consisting of the Information Systems Success Model and the Organizational Learning Theory. In Section 3, the Dynamic Security Success Model is presented, explaining all model constructs and their effects. The underlying methodical approach of the literature review is outlined in Section 4. The results of this literature review (synthesis) are described in Section 5 as well as the research gaps and the research questions. Section 6 presents the overall conclusions of this paper.

# 2 THEORETICAL BACKGROUND

There exist different, recognized approaches for managing organizational information using security frameworks such as ISO/IEC standards (27000 series), COBIT, ITIL, etc. Those frameworks provide guidelines, best practices and control objectives in order to achieve information security.
Although, employees are recognized as a resource which has to be managed including training, awareness and competence within the ISO standard for example (ISO 2005), it is not clear which influence such measures have on the individual, whether those measures are usable or whether they may cause dissatisfaction and therefore lead to an unintended behavior (e.g. circumventing security) even weakening organizational security. Those conventional approaches mainly concentrate on a more technical level (Von Solms 2005), while the individual, behavioral level is not considered. It is necessary, to also include the user into the security design (Sasse et al. 2001) next to security goals and technology, because "the human factor is the Achilles heel of information security" (Gonzalez & Sawicka 2002:1). This means that although technology may be able to provide a secure organizational environment, the individual may be the weakest point by circumventing or incorrectly applying security measures. As the previously mentioned security frameworks do not or not sufficiently consider human behavior as a consequence of applied security measures, we propose the Dynamic Security Success Model, which combines the organizational as well as the individual effects of IT security measures. We briefly explain the Information Systems Success Model and the Organizational Learning Theory in the following, which we combine and adapt to construct the Dynamic Security Success Model (DSSM) in the next section.

## 2.1 Information Systems Success Model

The Information Systems Success Model (ISSM) of DeLone and McLean (1992, 2003) is an established IS theory that provides an integrated view on IS success by explaining the relationships between six of the most critical dimensions of success (Fig. 1): System Quality, Information Quality, Use, User Satisfaction, Individual Impact and Organizational Impact and their relationships to each other as depicted by arrows. This widely cited model is considered as a standard model in the field of information systems research for measuring success (DeLone & McLean 2002). It is particular applicable for the field of smartphone security, because it refers to the individual context: Security in general and smartphone security in particular highly depend on the behavior of individuals. This issue is represented by the dimension Individual Impact which directly influences the organization. A short description of the model components can be found in Table 1.

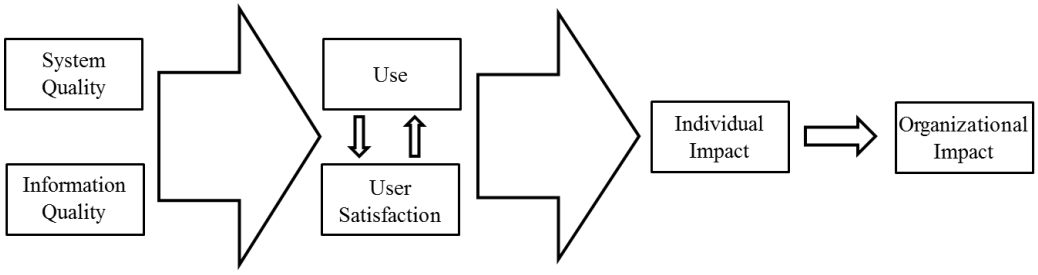


*Figure 1. DeLone's and McLean's Information Systems Success Model (Adapted from DeLone and McLean, 1992).*

In the ISSM, *System Quality* represents "the desired characteristics of the information system itself which produces information" (DeLone & McLean 1992:62). System Quality in the context of smartphone security could be measured by the flexibility of security measures, such as permitting the user to access corporate data from outside the company.
*Information Quality* concentrates on the information system output "namely, the quality of the information that the system produces, primarily in the form of reports" (DeLone & McLean 1992:64).

Examples for smartphone security are the policies and guidelines for employees explaining permitted and prohibited applications, e.g., white and black lists of apps.
The model component *Use* refers to the reported as well as to the actual usage of an information system and its output. *Use* in the smartphone security context refers to the activities the smartphone is used for, such as making phone calls and accessing corporate data under the condition of applied security measures which may restrain these activities.
*User Satisfaction* represents the interaction with the information system and evaluation whether this interaction is successful or not. In the context of smartphone security this means measuring employee satisfaction with smartphone use including the influence of security measures.
With the component *Individual Impact*, DeLone and McLean aim to measure the effect of the information system on the individual, e.g., regarding performance, which may also result in a changed organizational performance. Regarding smartphone security this means that for example, a positive effect of security measures on employee behavior, such as higher security awareness, may lead to a change in employee handling of data also regarding other corporate information systems. *Organizational Impact* consequently measures the effect of the information system on organizational performance. DeLone and McLean present several measures of *Organizational Impact* used by other authors including profit performance, profitability and overall cost-effectiveness of the information system. However, in the (smartphone) security context, quantifying the return on security investment is a challenging task (Böhme & Nowey 2008). An example for the *Organizational Impact* of smartphone security is the reduction or avoidance of mobile security breaches including loss of corporate data and money.

| **Construct** | **Description** | **Examples** |
|---|---|---|
| System Quality | Measurement of the quality of the information system | Reliability of virus scanner |
| Information Quality | Quality of the information system's output | Accuracy of biometric authentication, e.g. using fingerprint as authentication for the smartphone |
| Use | Usage of a system and its output | User scenarios, e.g. accessing the company's database from outside |
| User Satisfaction | User satisfaction with the system | Satisfaction with authentication policy, e.g. change of passwords every month |
| Individual Impact | Impact on individual behavior/performance | Security measures may increase the security awareness and behavior |
| Organizational Impact | Impact on organizational performance | Ensuring the confidentiality of corporate knowledge after a smartphone has been lost or stolen by a remote wipe function |

*Table 1. Description and Examples of Model Constructs of the ISSM according to DeLone and McLean 1992.*

## 2.2 Organizational Learning Theory

The Organizational Learning Theory is an established theory in the field of information systems which considers a company's ability to learn from mistakes and improve over time. This theory was developed by Chris Argyris whose representation plays a key role in the theory of how organizations learn. He defines organizational learning as the detection and correction of errors over time and describes individuals as agents whereby organizations learn through their agents (Argyris 1976). The schematic frame of the Organizational Learning Theory can be found in Figure 2 and a summary of the model components and their description is presented in Table 2.

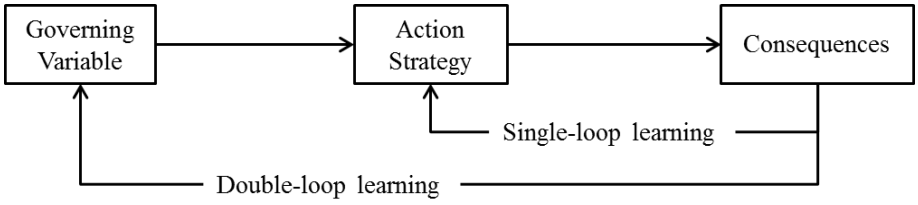


*Figure 2. Organizational Learning Theory (Adapted from Argyris, 1985).*

The model consists of three constructs (*Governing Variable, Action Strategy and Consequences*) as well as of two feedback loops (*Single-loop learning and Double-loop learning*). The *Governing Variable* represents a value which the company tries to satisfy and can be interpreted "as a continuum with a preferred range" (Argyris et al. 1985:84). Examples for *Governing Variables* in our scenario for smartphone security could be the confidentiality of organizational data, while the continuum could be represented by a classification scheme for different data. The *Action Strategy* is a "sequence of moves" which is used to satisfy the *Governing Variables* by obtaining intended *Consequences* (Argyris 1976). In our case, an *Action Strategy* could be organizing workshops for employees about selecting safe passwords for their smartphones. The chosen *Action Strategy* results in *Consequences* for the company which can be intended or unintended, as well as positive or negative for the organization. Consequences could be less security incidents or higher costs for security measures. In order to learn from past mistakes or to improve consequences, the company uses one of the two learning strategies: *Single-loop learning* is the simplest and most common learning technique and only changes the *Action Strategy* without critical refection. *Double-loop learning* is a more complex approach and means the re-evaluation of the goals and circumstances by considering the current *Governing Variables* (Argyris 1976).

The Organizational Learning Theory is suited for our literature review on smartphone security because (1) it is an established IS theory which considers the company's ability to learn from the past; (2) it has been already used for literature reviews (e.g. Wang & Ahmed 2003) and (3) it has been already used in connection with information security for example by Van Niekerk and von Solms (2004). These authors define the *Governing Variable* regarding information security as an acceptable level of risk. *Action Strategies* are defined as procedures which guide employee behavior in specific scenarios. The *Consequences* are the outcome of the *Action Strategies* including intended and unintended results.

| **Construct** | **Description** | **Examples** |
|---|---|---|
| Governing Variable | Defined values or goals which should be reached (Argyris et al. 1985) | Security goals of the company concerning the usage of smartphones e.g. consideration of legal conditions |
| Action Strategy | Measures taken in order to satisfy the defined values and goals (Argyris et al. 1985) | Password policies to control user access to the smartphone and to corporate data |
| Consequences | Results of the action strategy; can be intended or unintended (Argyris et al. 1985) | Decrease of work performance, less security breaches |
| Single-loop learning | Adjustment of unintended consequences by changing the action strategy (Tagg 2010) | Increase of password expiration periods to decrease user authentication effort |
| Double-loop learning | Adaption of the governing variable due to a change of circumstances in order to achieve intended consequences (Tagg 2010) | Adaption of security goals due to changed legal conditions |

*Table 2. Description and Examples of Model Constructs of the Organizational Learning Theory.*

# 3 DYNAMIC SECURITY SUCCESS MODEL

We combined the Organizational Learning Theory and the Information Systems Success Model and adapted it resulting in the Dynamic Security Success Model (DSSM). Literature reviews using a combination of models have already been realized, e.g. by Weishäupl et al. (2015). The model is displayed in Figure 3 and the constructs and effects are explained in the following and summarized in Table 3. The aim of the Dynamic Security Success Model is to associate the effects of individual consequences with the effects of organizational consequences regarding smartphone use and smartphone security measures. This also includes feedback loops aiming to generate knowledge and learn from experiences with individual and organizational consequences of security measures. The boundary conditions of our model are organizations (1) with employees using smartphones for business purposes and (2) having organizational and/or technical security measures for smartphones in place. The model is independent of the smartphone integration concept, meaning whether a "bring your own device" policy is in place or whether corporate owned devices are used or any hybrid form.
The Organizational Learning Theory has the advantage to observe whether taken actions cause intended Consequences and if not result in a change of the Action Strategy or of the Governing Variable respectively. The advantage of the Information Systems Success Model is the more fine-grained view including both, Individual and Organizational Impacts. The new model combines the advantages of both theories: the characteristics of the individual context and the possibility and dynamic to learn from feedback.

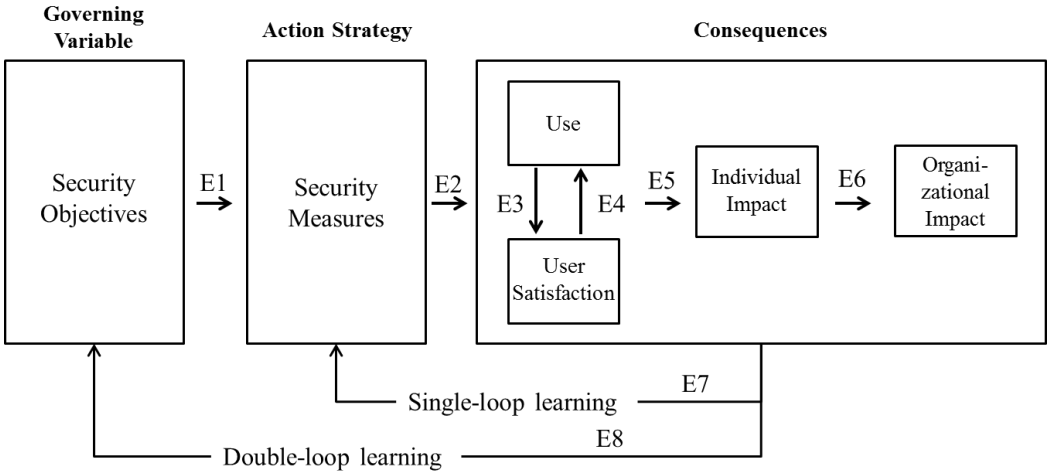


*Figure 3. Dynamic Security Success Model based on DeLone and McLean (1992) and Argyris (1976).*

## 3.1 Model constructs

We interpret the dimensions System Quality and Information Quality of the ISSM as reliability and accuracy of security measures based on the findings of DeLone & McLean (1992). The quality of security is dependent and influenced by further factors (framing conditions) such as the company size, the data processed within the company, the underlying attacker model, etc. Therefore, it is necessary to consider the aspect of quality together with the framing conditions. This is the reason for adapting the presentation of System and Information Quality of the original ISSM. We do not drop the effect of System and Information Quality on Use and on User Satisfaction. Instead we extend the construct resulting in the Security Objective construct. Although indirect, the relationship of the Quality dimension and Use/User Satisfaction still exists in our model.
The Action Strategy is represented by the applied security measures, for example the establishment of policies relating to the usage of smartphones for employees. The constructs Use, User Satisfaction, Individual Impact and Organizational Impact can be modelled as Consequences for the organization.

The Governing Variable, as well as the Action Strategy, refer to security related issues only, while the Consequences also cover non-security related topics. The restriction for the Governing Variable and for the Action Strategy provides the framework regarding security aspects of smartphones in companies. The Consequences are interpreted more broadly in favor of also revealing non-security related implications of smartphones in general and of security measures in particular. In compliance with the Information Systems Success Model, relationships between the constructs symbolize the impact or effect on another construct, e.g., security objectives of a company are implemented in security measures such as using Mobile Device Management software to manage smartphones. These effects are displayed as arrows in the model presentation (E1-E8) and are described in the following.

### 3.2 Relationships between the constructs

**E1:** Security Objectives refer to issues related to the integration of smartphones into organizations, e.g., confidentiality and availability of organizational data. Security Objectives determine which security measures are applied within a company. The effects of the Security Measures on employees and on the whole company are summarized within the Consequences part of our model.
**E2:** Security Measures are implemented in order to fulfill the Security Objectives and goals of a company. An example for such strategies is the enforcement of smartphone disc encryption. According to Van Niekerk and von Solms (2004), security controls can be divided into physical, technical and operational controls. Physical controls refer to physical security such as a lock on the door. Technical controls refer to software based security solutions, e.g., the enforcement of user authentication by user name and password. Operational controls take the human behavior component into consideration by imposing behavioral rules, e.g., policies and guidelines defining password rules for authentication on the smartphone. Action Strategies lead to certain Consequences, which affect individuals (employees) and also the organization e.g., authentication policies (regular change of password) which lead to dissatisfaction among employees, reduce the use of smartphones and have a negative effect on working efficiency and on organizational performance.
**E3 + E4:** Use describes the tasks the smartphone is used for including the net benefit which is provided by the usage of these devices, for example being able to access corporate data at customer sides. User Satisfaction summarizes the responses of the employees to smartphone usage and to the applied smartphone security measures, for example being dissatisfied with the exclusion of private use on a company owned smartphone. Use and User Satisfaction mutually influence each other. For example, positive experiences with smartphone use can lead to a higher degree of satisfaction. Positive user satisfaction can then increase the use.
**E5:** The Individual Impact represents the effects of the smartphone integration including security related effects on the employees such as decreased working productivity due to authentication policies. Smartphone Use and User Satisfaction with the smartphone and the applied security measures have an impact on the individuals. This individual impact can be positive or negative. An example of a positive effect is increased security awareness affecting also the behavior of employees regarding other information systems. Examples for negative effects are security measures conflicting with work, when corporate emails are not allowed on the smartphone due to security policies.
**E6:** Organizational Impact describes the effects of smartphone integration, also including security related effects, on the company and on its performance, e.g., decrease of security risks by smartphones which are connected to the corporate network by means of applied security measures. The Individual Impact can lead to Organizational Impact when smartphone security measures are circumvented putting company data and knowledge at risk.
**E7 + E8:** Single-loop learning within a company occurs when the Action Strategy has to be adapted. In the smartphone context this means that the consequences generated an unintended outcome to which the company should react to, e.g., when security policies and procedures limit the functionality of smartphones to being able to make phone calls only. These security measures limit the smartphone integration in a way which may not be intended and consequently would lead to an adaption of the policies. Double-loop learning occurs when the framework conditions of the company have changed, e.g., due to a change of legal regulations, which results in an adjustment of the security objectives.

| Construct | Description | Example |
|---|---|---|
| **Governing Variable** | | |
| Security Objectives | Enterprise security goals related to smartphone integration into the company network | Ensure confidentiality, integrity and availability of corporate information (Copeland & Chiang 2012); Legal regulations in the EU e.g., General Data Protection Regulation concerning smartphone policies (Samaras et al. 2014) |
| E1 | Effect of the security objectives on the applied security measures | To fulfill legal requirements, organizations have to implement security controls (Samaras et al. 2014) |
| **Action Strategy** | | |
| Security Measures | Security measures and controls used to protect access to smartphones and their data and information resources, e.g., technical and operational controls (Van Niekerk and Von Solms, 2004) | Introducing security policies and software on smartphones to enforce policies such as MDM software; appliance of security awareness training; mobile device risk assessment and management (Patten et al. 2013) |
| E2 | Effect of applied security measures on the individual and organizational consequences | Authentication procedures (Samaras et al. 2014) can decrease user satisfaction and lead to circumventing security measures putting organizational data at risk |
| **Consequences** | | |
| Use | Operation purposes and actual usage of smartphones in a business context | Management of information, e.g., contact details and appointment (Verma et al. 2011); share files and data (Chaudhry 2012) |
| User Satisfaction | Employees' work satisfaction with smartphones, smartphone usage and with smartphone security measures | Security policies negatively influence mobile device usability (Rubin et al. 2013) |
| E3 | Effect of Use on User Satisfaction | Positive experiences with smartphone use can lead to a high degree of work satisfaction (Harris et al. 2012); Convenience increases with the use of smartphones by being able to connect to the internet easily (Chigona et al. 2012) |
| E4 | Effect of User Satisfaction on Use | Positive user satisfaction with security policies can increase the actual usage (Landman 2010) |
| Individual Impact | Impact of smartphones and security related impact on employees, e.g., regarding work efficiency | Employees are connected to their office and available anytime which improves working efficiency (Rubin et al. 2013) |
| E5 | Effect of Use and User Satisfaction on Individuals | Use and user satisfaction influence the degree to which smartphones are used and therefore influence the working efficiency |
| Organizational Impact | Impact of smartphones and security related impact on the company, e.g., increase of business operations, increase of data security | Reduced risk of lost or stolen smartphones causing security breaches and leading to costs (Landman 2010) |
| E6 | Effect of Individuals on the Organization | Increased security awareness through smartphone security measures may increase the company's overall security |
| **Feedback** | | |
| Single-loop learning / E7 | Adaption of action strategy due to unintended consequences | Applied security measures can lead to a restriction of smartphone functionality which negatively affects its benefit (Rubin et al. 2013), making an adaption necessary |
| Double-loop learning / E8 | Adaption of governing variable due to changed framework conditions | Changes of legal regulations affecting the security objectives resulting in its adaption |

*Table 3. Description and Examples of Model Constructs of the DSSM.*

# 4 RESEARCH METHODOLOGY

We conducted a structured literature review according to Okoli and Schabram (2010). We developed and tested a protocol including research questions, search strategy, practical screen, quality appraisal and data extraction strategy. Upon request, the complete protocol can be obtained from the authors.
For our research, we selected appropriate electronic databases including peer-reviewed leading journals and conference proceedings, because these sources include the major contributions (Webster & Watson, 2002). We refined the selection by analyzing the editorial statements. Databases which were included are: ACM Digital Library, IEEE Xplore Digital Library, Ebsco Host Business Source Complete, Ebsco Host Business Source Premier and AIS Electronic Library. We further searched within Science Direct und Google Scholar to complete the search. Levy and Ellis (2006) propose a forward and backward search due to "the diversification and multidisciplinary nature of IS literature" (p. 189) in order to extend the search. Therefore, we checked the references of the identified articles and used Google Scholar to find relevant articles citing our identified papers (backward and forward search according to Webster and Watson 2002). The backward search revealed 37 additional results and the forward search revealed 15 additional results. Our literature search revealed 569 papers in total. We did not limit the time covered for our search. A keyword search was used on the titles and the abstracts by developing a Boolean search string[1]. Keywords were chosen according to our model. We included both, articles dealing with company owned smartphones as well as with personally owned devices. According to our defined inclusion and exclusion criteria for content and quality (practical screen and quality appraisal pilot tested and defined in the literature protocol), a subset of the initially 569 articles was identified. One reviewer therefore read all titles and abstracts, while a second independent reviewer analyzed a 10% sample of the 569 identified articles. The sample was randomly chosen among all articles and databases. Papers which focused on risk assessment of smartphones in companies were excluded, e.g., Yazid et al. (2012). We further excluded papers which deal with smartphone security and privacy aspects for private usage as well as papers dealing with smartphone security and technical frameworks, e.g. Lo et al. (2008).
The Kappa statistic was used to measure interrater reliability as suggested by Fink (2013), who recommends aiming for a kappa between 0.6 and 1.0. Agreement between the two reviewers whether to exclude or include an article in the literature review reached a kappa value of 0.6 for the 10% sample. After this identification phase, two reviewers read all remaining 95 articles in detail in order to determine their inclusion in the review. Disagreement was resolved by discussion. Relevant data was extracted into a coding sheet, independently performed by the two reviewers. For the data extraction phase, 74 articles were considered. Finally, a synthesis was developed revealing research gaps. The structured literature review was an exhaustive search with selective citation due to lack of space.

# 5 SYNTHESIS AND IDENTIFICATION OF RESEARCH GAPS

In the following section we present the results of the synthesis phase of our literature review. The presentation of the results is structured according to the previously introduced Dynamic Security Success Model (Figure 3). We conclude each subsection with the identification of research gaps as recommended by Webster and Watson (2002) and therefore formulate research questions for the effects E1 to E8.

[1] (enterprise OR firm OR company OR organization OR employee) AND (smartphone OR "smart phone" OR "smart phones" OR "mobile device" OR "mobile devices" OR "mobile phone" OR "mobile phones") AND (security OR secure OR attack OR risk OR breach OR protect OR misuse).

### 5.1 Effect of Security Objectives on Security Measures (E1)

Security Objectives refer to enterprise security goals concerning the smartphone integration into a company network. These security goals relate to the protection of corporate information stored on and being accessible by the smartphones and the company's network as well (Barr et al. 2010). The focus is on the protection of sensitive corporate information and services, while ensuring confidentiality, integrity and availability (Sari et al. 2014; Mazhelis et al. 2007). These sensitive information need to be protected against unauthorized access in case of loss or theft of the device itself (Wright Jr et al. 2011). The importance of securing access to this sensitive information depends on the specifications made in the Security Objectives, i.e., the more likely an attack on corporate information, the stronger security measures have to be applied. Consequently, information security is part of the Security Objectives. According to von Solms, "the aim of information security is to ensure business continuity and [to] minimize business damage by preventing and minimizing the impact of security incidents" (von Solms, 1998, p. 224).
Security Objectives are subject to a wide range of influences such as legal regulations, the knowledge and education of employees regarding security, the sensitivity of corporate data and the likelihood of an attack. Samaras et al. (2014) describe the legal conditions for organizations located in the EU. The (planned) General Data Protection Regulation (GDPR) forms the framework for the processing of personal data. Whenever personal (employee) data and corporate data are mixed, e.g., when introducing bring your own device (BYOD) policies, the organization has to ensure that these sensitive information are secure by installing appropriate security controls. Otherwise, the organization can be made responsible for data breaches. These legal regulations differ between countries and have to be considered when integrating smartphones and applying related security measures. Organizations not only are subject to different legal constraints, but also to different potential threats. To minimize the potential damage for a company, appropriate Security Measures and tools have to be developed, including information security management (Sari et al. 2014; Copeland & Chiang 2012). Literature dealing with the knowledge and education of employees regarding security issues in organizations or for the influence of the sensitivity of corporate data on Security Measures is rare. The research questions we focus on are therefore: **What are the Security Objectives that influence the company's decisions regarding smartphone security? How are Security Measures derived from these Security Objectives?**

### 5.2 Effect of Security Measures on the Consequences (E2)

Most articles do not put major focus on the effect of applied Security Measures for smartphones on the Consequences for the individual and the company. Landman (2010) describes the conflict between security and efficiency, which describes a tradeoff: implementing effective security procedures mutually exclude efficient business operations and high employee acceptability. Usability may also be reduced as a consequence of protection measures (Rubin et al. 2013), for example by introducing time-consuming security policies for user authentication. However, papers dealing with the effect of Security Measures on Use of smartphones in organizations and on User Satisfaction of employees are rare. We therefore formulate the following research question: **What are the consequences of applied Security Measures on the Use and on User Satisfaction of employees?**

### 5.3 Effect of Use on User Satisfaction and vice versa (E3+E4)

The model component Use refers to the operation purposes and to the actual use of smartphones in the business context. We do not regard Use in direct correlation with security measures, as their usage is not voluntarily (DeLone & McLean 1992). We found many papers describing the areas of applications, e.g., using email and calendar applications (Kodeswaran et al. 2012; Jacoby et al. 2007; Disterer & Kleiner, 2013), accessing and sharing company files and data (Russello et al. 2012; Smaldone et al. 2009; Bernik & Markelj 2012; Chigona et al. 2012; Chaudhry 2012; Disterer &

Kleiner 2013) and conducting traditional telephone communication including phone calls and short text messages (Disterer & Kleiner 2013; Sun et al. 2013; Parham et al. 2015). We only found very few papers dealing with the effect of Use on User Satisfaction. Scarfo (2012) claims that User Satisfaction increases, when employees are allowed to use their personal devices. The possibility to choose the devices themselves increases the opportunities to collaborate and consequently increases User Satisfaction. Eslahi et al. (2014) also state that personal devices used in a company context can increase User Satisfaction. Chigona et al. (2012) describe that employees feel more convenient when using smartphones for work, due to the possibility of easy internet access. The effect of User Satisfaction on smartphone Use could only be identified in the paper of Idemudia et al. (2014). The authors developed a model based on the visual perception theories in order to understand the factors influencing smartphone use at the individual level in organizations. They concluded that 79% of smartphone use can be explained with users being familiar with a smartphone and with cognitive trust in the integrity of a smartphone (Idemudia et al. 2014). However, the effect of employee satisfaction on applied security measures is not covered by the literature yet. The following research questions thus need further investigation: **How does smartphone Use influence User Satisfaction? How does User Satisfaction with smartphone Security Measures affect actual usage?**

### 5.4 Effect of Use and User Satisfaction on Individual Impact (E5)

Individual Impact is being directly affected by Use and User Satisfaction. We identified both positive and negative consequences for the employees. Using smartphones in organizations has a positive impact on employee's productivity and efficiency (Sun et al. 2013; Rubin et al. 2013) enabling an increase of 40% in productivity (Wright Jr et al. 2011). The reasons for this increase is due to being always updated while on the move (Zhauniarovich et al. 2014) and to work location-independent (Gheorghe & Neuhaus 2013) by sharing data and collaborate on these files with colleagues and customers (Chaudry 2012; Chigona et al. 2012). Smartphones also lead to a higher flexibility (Eslahi et al. 2014) and availability (Milligan 2008) by being able to conduct business more flexibly (Copeland & Chiang 2012) and improve turnaround times for problem resolution (Wright Jr et al. 2011). These positive consequences are not related to security measures but to advantages of smartphones in organizations in general. As we stated in the beginning, we are not only interested in security related, but also in non-security related consequences. However, information on the positive effect of security measures on smartphones for the individual e.g., causing employees to feel more secure or increasing security awareness is scarce.

Negative consequences of smartphone integration into the business context are especially related to the BYOD solutions. Allowing employees to use their own personal devices for business purposes increases the workload for the IT department (Allam & Flowerday, 2011) as it becomes necessary to cover a wide range of different devices concerning threat detection and threat mitigation mechanisms (Peng et al. 2013; Scarfo 2012; Koch & Curry 2014). This approach can also be negative for the employees as personal devices lead to a constantly accessible workforce resulting in higher stress levels (Ortbach et al. 2013). The BYOD approach can also be invasive of employee's privacy (Peng et al. 2013; Chigona et al. 2012) as security mechanisms may enable the employer to monitor the personal device and track the employee's location for example (Totten & Hammock 2014). Our research question to address this issue is: **What are positive as well as negative consequences of security measures for individuals in organizations?**

Independent of the smartphone integration approach (device personally owned or company owned), security measures can lead to a decrease in productivity (Allam & Flowerday 2011) when authentication policies prescribe a high complexity for passwords which increases the workload and equally decreases productivity. The effect of User Satisfaction with smartphones in general and with applied smartphone Security Measures in particular on employees are not dealt with in literature, resulting in the research question: **How does User Satisfaction with smartphones and with smartphone Security Measures influence individuals?**

### 5.5 Effect of Individual Impact on Organizational Impact (E6)

Individual Impact of smartphones in organizations is directly related to the Organizational Impact. This means that all advantages and disadvantages for the individuals directly affect the organization. The articles analyzed revealed both positive and negative consequences for the organization. The possibility to access current customer information via smartphone independently from the employee's location accelerates the process of responding to customer needs and therefore leads to a significant improvement of customer satisfaction (Wright Jr et al. 2011). Smartphones and smartphone apps enable more productive business processes e.g., within inventory management or technical support (Waterfill & Dilworth 2014). From the point of view of the company, it is beneficial when employees use their personal smartphones for business purposes because they are always accessible, even outside working hours, building a constantly connected workforce (Olalere et al. 2015; Allam et al. 2014). However, it is unclear whether this argument is exclusively positive, as constant accessibility may also have negative effects such as stress for the individual (Ortbach et al. 2013) and consequently may lead to negative effects for the company as well. Russello et al. (2012) argues that despite the benefits of increasing productivity when using smartphones, companies have to consider that corporate data is vulnerable to malicious applications leaking sensitive data. These security issues, including loss of data and data being compromised can result in decreased market shares (Green 2007) and consequently in loss of money (Landman 2010). This risk is particular severe for the BYOD solution, where employees may be confronted with situations involving external services over an external network and may not have the adequate level of awareness and knowledge to configure their device appropriatly (Allam & Flowerday 2011).

The most often mentioned effect on the organization is the increase of employees' productivity. However, papers describing the measurement of the increase in productivity when using smartphones in organizations are scarce at best as well as a description of how security measures affect this increase in productivity. It is not clear to what extent security measures on the one hand affect individuals and on the other hand affect the organization. These influences can be positive (reduce or avoid security breaches) or negative (increased workload leading employees to circumvent security measures and decreasing organizational security). Brodin et al. (2015) suggest research directions for BYOD management issues including developing methodologically techniques to measure the influence of smartphones on personal productivity. The authors point out that a lot of previous research on this topic was conducted by large industry players (Intel and Cisco) who are interested in promoting the BYOD approach. Therefore, independent research is proposed for evaluating the benefits and costs of smartphones in companies (Brodin et al. 2015). We extend this proposal by including the security perspective in the evaluation for smartphones in organizations. This leads us to the following research question: **How does the Individual Impact of smartphone security measures affect the organization?**

### 5.6 Effect of Single-loop learning (E7)

Single-loop learning within a company takes place when the action strategy has to be adapted. This can be the case when the consequences contradict the original goal. As an example for Single-loop learning one can think of security policies for user authentication on smartphones. If these policies prescribe a periodically change of passwords e.g., every month, employees may tend to reuse passwords or use weaker passwords if possible. Therefore, the intended consequence of the Security Measure authentication policy may not be reached. Instead, the measure might reduce IT security. As a result, this Security Measure has to be adapted to achieve the intended security goal. Another example for Single-loop learning is the possibility to share corporate data. If it is prohibited to save corporate data on the smartphone, employees may circumvent this security measure by using file hosting services such as Dropbox. This can lead to uncontrolled access of corporate data and is not intended by the security measure. Unintended positive consequences are also a conceivable outcome. Employees may feel more secure when appropriate security measures are applied. This can lead to higher user satisfaction and increase the possibility that employees follow security guidelines of other

information systems. We propose the following research question: **How can a company learn from the consequences of past smartphone security measures and incidents in the future through Single-loop learning?**

### 5.7 Effect of Double-loop learning (E8)

Double-loop learning indicates a re-evaluation of the goals and circumstances by considering the current governing variables (Argyris 1976). A re-evaluation may become necessary, when the factors which determine the governing variables have changed, e.g., the legal regulations. Mattia and Dhillon (2003) describe the importance of Double-loop learning regarding security in organizations. They state that a result of Double-loop learning is an increased effectiveness in decision making leading to effective security within the company. We found evidence that Security Measures have to be constantly adapted. This necessity results from the changes in smartphone operating systems (e.g., Android, iOS, BlackBerryOS), from application development and also from mobile threats (Li & Clark 2013), whereas the latter such as malware is probably the greatest issue for adaption. Yu et al. (2013) present a threat monitoring system in order to reveal threats for mobile devices in organizational networks. The system was developed to detect malware on Android devices including unknown malware detection by applying machine learning algorithms. This research indicates that approaches for Double-loop learning already exist by responding to changes from the outside. In view of the analyzed literature, we propose the following research questions: **When is Double-loop learning more appropriate than Single-loop learning? How does Double-loop learning affect an organization's security regarding smartphones?**

## 6 CONCLUSION

We contribute to the IS research community by developing the Dynamic Security Success Model, which is a combination of the Organizational Learning Theory (Argyris 1976) and the Information System Success Model of DeLone and McLean (1992). The model includes a fine-grained view of the effects of individual and organizational impacts regarding smartphone security measures on the organization. It also includes the dynamic to learn according to feedback, either by adapting the action strategy or if necessary the governing variable. On the basis of this model, we further present a structured and exhaustive literature review (according to Okoli and Schabram, 2010), which synthesizes literature on smartphone security in organizations. For reasons of brevity, we highlight the most interesting aspects. We finally included 74 relevant articles in our review and presented the results in a concept-centric way structured by our introduced Dynamic Security Success Model as suggested by Webster and Watson (2002). We conclude each presentation of the model components and their effects on each other with the identification of research gaps in order to point out directions for future work. Although, we applied a structured approach, we might have missed relevant articles in our literature review. This may be also owed to the fact that the number of selected sources (journal and conference proceedings) was limited.

Regarding the synthesis of our literature review, we will concentrate our future research on the identified research gaps, especially single-loop and double-loop learning of organizations according to the consequences of smartphone security measures. This learning process is probably the most important aspect for organizations in order to stay competitive and secure information and knowledge as the field of IT security is subject to constant change. Therefore, we will collect data in organizations that have integrated smartphones for business purposes. We are currently conducting explorative expert interviews with IT security manager of different large German companies in order to evaluate the feasibility of our model. These results will enrich the model and will be further evaluated in a case study approach. We hope that this literature review stimulates future academic research in the field of smartphone security while given an overview on smartphone security research for practitioners.

## ACKNOWLEDGEMENT

The research leading to these results was supported by the "Bavarian State of Ministry, Education, Science and the Arts" as part of the FORSEC research association (https://www.bayforsec.de).

## References


Allam, S. and Flowerday, S. (2011). An Adaptation of the Awareness Boundary Model towards Smartphone Security. Information Security South Africa (ISSA).

Allam, S., Flowerday, S.V. and Flowerday, E. (2014). Smartphone Information Security Awareness: A Victim of Operational Pressures. Computers & Security 42, pp. 56-65.

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

Argyris, C., Putnam, R. and Smith, D.M. (1985). Action Science. San Francisco, Jossey-Bass Publisher.

Barr, K. et al. (2010). The VMware Mobile Virtualization Platform: Is that a Hypervisor in Your Pocket?. ACM SIGOPS Operating Systems Review 44(4), 124-135.

Bernik, I. and Markelj, B. (2012). Blended Threats to Mobile Devices on the Rise. International Conference on Information Society (i-Society), pp. 59-64.

Böhme, R. and Nowey, T. (2008). Economic Security Metrics. Dependability Metrics. Ed. By Eusgeld, I., F.C. Freiling and R. Reussner. Berlin Heidelberg: Springer Verlag, pp. 176-187.

Brodin, M., Rose, J. and Åhlfeldt, R.M. (2015). Management Issues for Bring Your Own Device. European, Mediterranean & Middle Eastern Conference on Information Systems 2015 (EMCIS2015), pp. 1-12.

Chaudhry, P. (2012). Tech Strategy-Needed: A Corporate Mobile Device Policy. Financial Executive-Magazine of Financial Executive Institute 28(5), 69.

Chigona, W., Robertson, B. and Mimbi, L. (2012). Synchronised Smart Phones: The Collision of Personal Privacy and Organisational Data Security. South African Journal of Business Management 43(2), 31-40.

Copeland, W. and Chiang, C. (2012). Securing Enterprise Mobile Information. Computer, Consumer and Control (IS3C), 2012 International Symposium, pp. 80-83.

DeLone, W. H. and McLean, E.R. (1992). Information Systems Success: The Quest for the Dependent Variable. Information Systems Research, 3(1), 60-95.

DeLone, W. H. and McLean, E.R. (2002). Information Systems Success Revisited. System Sciences (HICSS), 2002. Proceedings of the 35th Annual Hawaii International Conference. IEEE, pp. 2966-2976.

DeLone, W. H. and McLean, E.R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-year Update. Journal of Management Information Systems, 19(4), 9-30.

Disterer, G. and Kleiner, C. (2013). "BYOD-Bring Your Own Device." HMD Praxis der Wirtschaftsinformatik, 50(2), 92-100.

Eslahi, M. et al. (2014). BYOD: Current State and Security Challenges. In: Symposium on Computer Applications and Industrial Electronics (ISCAIE), pp. 189-192.

Fink, A. (2013). Conducting Research Literature Reviews: From the Internet to Paper. Sage Publications.

Gartner (2013). Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes. URL: http://www.gartner.com/newsroom/id/2466615 (visited on 03/11/2016).

Gheorghe, G. and Neuhaus, S. (2013). Poster: Preserving Privacy and Accountability for Personal Devices. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM, pp. 1359-1362.

Gonzalez, J. J. and Sawicka, A. (2002). A framework for human factors in information security. Wseas international conference on information security, Rio de Janeiro, 2002.

Green, A. (2007). Management of Security Policies for Mobile Devices. Proceedings of the 4th Annual Conference on Information Security Curriculum Development. ACM, p. 22.

Harris, J., Ives, B. and Junglas, I. (2012). IT Consumerization: When Gadgets Turn into Enterprise IT Tools. MIS Quarterly Executive 11(3), 99-112.

Idemudia, E. C., Raisinghani, M.S. and Batch, A. (2014). Empirical Investigation of the Cognitive Factors that Influence the Continued Use of Smartphones by College Students Who are Using

Smartphones to Participate in the Future Global Distributed Teams. System Sciences (HICSS), 2014, 47th Hawaii International Conference. IEEE, pp. 289-299.
Jacoby, G. A., Ransbottom, J.S., Hickman, T. and Potasznik, M. (2007). Screening Mobile Devices to Examine Network Health. System Sciences (HICSS), 2007. Proceesings of the 40th Annual Hawaii International Conference. IEEE, pp. 164-172.
ISO. (2005). Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC FDIS 27001:2005(E).
Koch, H. and Curry, P. (2014). IT Consumerization's Impact on Enterprise IT. Twentieth Americas Conference on Information Systems, pp. 1-11.
Kodeswaran, P., Nandakumar, V., Kapoor, S., Kamaraju, P., Joshi, A. and Mukherjea, S. (2012). Securing Enterprise Data on Smartphones Using Run Time Information Flow Control. Mobile Data Management (MDM), IEEE 13th International Conference. IEEE, pp. 300-305.
Landman, M. (2010). Managing Smart Phone Security Risks. 2010 Information Security Curriculum Development Conference. ACM, pp. 145-155.
Levy, Y. and Ellis, T. J. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. Informing Science: International Journal of an Emerging Transdiscipline, 9(1), 181-212.
Li, Q. and Clark, G. (2013). Mobile Security: A Look Ahead. Security & Privacy, IEEE 11(1), 78-81.
Lo, J. L., Bishop, J. and Eloff, J.H.P. (2008). SMSSec: An End-to-end Protocol for Secure SMS. Computers & Security 27(5), 154-167.
Mattia, A. and Dhillon, G. (2003). Applying Double Loop Learning to Interpret Implications for Information Systems Security Design. Systems, Man and Cybernetics. IEEE International Conference, pp. 2521-2526.
Mazhelis, O. and Puuronen, S. (2007). A Framework for Behavior-based Detection of User Substitution in a Mobile Context. Computers and Security 26(2), 154-176.
Milligan, P. M. and Hutcheson, D. (2008). Business Risks and Security Assessment for Mobile Devices. Information Systems Control Journal 1, p. 24.
Mistiaen, P., Francke, A.L. and Poot, E. (2007). Interventions Aimed at Reducing Problems in Adult Patients Discharged from Hospital to Home: A Systematic Meta-review. BMC Health Services Research, 7(1), 47.
Mylonas, A., Dritsas, S., Tsoumas, V. and Gritzalis, D. (2011). Smartphone security evaluation the malware attack case. Security and Cryptography (SECRYPT). Proceedings of the International Conference on. IEEE, pp. 25-36.
Okoli, C. and Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. Sprouts: Working Papers on Information Systems, 10 (26).
Olalere, M., Abdullah, M.T., Mahmod, R. and Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. URL: http://sgo.sagepub.com/content/5/2/2158244015580372/ (visited on 11.10.2015).
Ortbach, K., Köffer, S., Müller, C.P.F. and Niehaves, B. (2013). How IT Consumerization Affects the Stress Level at Work: A Public Sector Case Study. PACIS, p. 231.
Parham, A. G., Mooney, J.L. and Cairney, T.D. (2015). When BYOD Meets Big Data. Journal of Corporate Accounting & Finance 26(5), 21-27.
Patten, K. P. and Harris, M.A. (2013). The Need to Address Mobile Device Security in the Higher Education IT Curriculum. Journal of Information Systems Education 24(1), 41.
Peng, W., Li, F., Han, K.J., Zou, X. and Wu, J. (2013). T-dominance: Prioritized Defense Deployment for BYOD Security. Communications and Network Security (CNS), 2013 IEEE Conference. IEEE, pp. 37-45.
Rubin, Y., Guy, N., Shachor, G., Kallner, S. and Ben-Harrush, I. (2013). Puremeap - A Mobile Enterprise Application Platform: A Bird's-eye View of the Software Architecture. In: Proceedings of the 2013 ACM Workshop on Mobile Development Lifecycle. ACM, pp. 17-18.
Russello, G., Conti, M., Crispo, B. and Fernandes, E. (2012). MOSES: Supporting Operation Modes on Smartphones. Proceedings of the 17th ACM Symposium on Access Control Models and Technologies. ACM, pp. 3-12.

Samaras, V., Daskapan, S., Ahmad, R. and Ray, S.K. (2014). An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD. Telecommunication Networks and Applications Conference (ATNAC), Australasian. IEEE, pp. 129-134.

Sari, P. K. and Trianasari, N. (2014). Information Security Awareness Measurement with Confirmatory Factor Analysis. Technology Management and Emerging Technologies (ISTMET), 2014 International Symposium. IEEE, pp. 218-223.

Sasse, M. A., Brostoff, S. and Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT technology journal 19(3), (2001), 122-131.

Scarfo, A. (2012). New Security Perspectives around BYOD. In: Proceedings of the 7th International Conference on Broadband, Wireless Computing, Communication and Applications, BWCCA. IEEE, pp. 446-451.

Seddon, P. B. (1997). A Respecification and Extension of the DeLone and McLean Model of IS Success. Information Systems Research, 8(3), 240-253.

Smaldone, S., Ganapathy, V. and Iftode, L. (2009). Working Set-based Access Control for Network File Systems. Proceedings of the 14th ACM Symposium on Access Control Models and Technologies. ACM, pp. 207-216.

Sun, Q., Qi, T., Yang, T. and Cui, Y. (2013). An Android Dynamic Data Protection Model Based on Light Virtualization. Communication Technology (ICCT), 2013 15th IEEE International Conference. IEEE, pp. 65-69.

Tagg, J. (2010). The Learning-paradigm Campus: From Single-to Double-loop Learning. New Directions for Teaching and Learning, 123, pp. 51-61.

Totten, J. A. and Hammock, M. (2014). Personal Electronic Devices in the Workplace: Balancing Interests in a BYOD World. ABA Journal of Labor & Employment Law, 30(1), 27-45.

Van Niekerk, J. and von Solms, R. (2004). Organisational Learning Models for Information Security. In: The ISSA 2004 Enabling Tomorrow Conference, p. 30.

Verma, R., Tomar, D.S. and Rathore, S.K. (2011). Extraction and Verification of Mobile Message Integrity. Communication Systems and Network Technologies (CSNT), 2011 International Conference. IEEE, pp. 49-53.

Von Solms, R. (1998). Information Security Management (3): The Code of Practice for Information Security Management (BS 7799). Information Management & Computer Security, 6(5), 224-225.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both?. Computers & Security 24.2 (2005): 99-104.

Wang, C. L. and Ahmed, P.K. (2003). Organisational Learning: A Critical Review. The Learning Organization, 10(1), 8-17.

Waterfill, M. R. and Dilworth, C.A. (2014). BYOD: Where the Employee and the Enterprise Intersect. Employee Relations Law Journal, 40(2), 26-36.

Webster, J. and Watson, R.T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. Management Information Systems Quarterly, 26(2), 3.

Weishäupl, E. and Yasasin, E. and Schryen, G. (2015). A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory. International Conference on Information Systems, December 13-16, 2015, Fort Worth, Texas, USA.

Wright Jr, H. R., Mooney, J.L. and Parham, A.G. (2011). Your Firm's Mobile Devices: How Secure are they?. Journal of Corporate Accounting & Finance, 22(5), 13-21.

Yazid, S. A. I. et al. (2012). Enhancement of Asset Value Classification for Mobile Devices. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference. IEEE, pp. 106-110.

Yu, W., Chen, Z., Xu, G., Wie, S. and Ekedebe, N. (2013). A Threat Monitoring System for Smart Mobiles in Enterprise Networks. Proceedings of the 2013 Research in Adaptive and Convergent Systems. ACM, pp. 300-305.

Zhauniarovich, Y., Russello, G., Conti, M., Crispo, B. and Fernandes, E. (2014). MOSES: Supporting and Enforcing Security Profiles on Smartphones. Dependable and Secure Computing, IEEE Transactions, IEEE, 11(3), 211-223.