Postprint of the paper published in IJESMA:
Hustad, E., Bekkevik, F. M., Holm, O. R., & Vassilakopoulou, P. (2020). Employee Information Security Practices: A Framework and Research Agenda. *International Journal of E-Services and Mobile Applications (IJESMA)*, *12*(2), 1-14.

Employee Information Security Practices: A Framework and Research Agenda

Eli Hustad, *University of Agder, Norway*

Frode Mathias Bekkevik, *Evry, Norway*

Ole Reidar Holm, *Bekk, Norway*

Polyxeni Vassilakopoulou, *University of Agder, Norway*

ABSTRACT

Employee information security practices are pivotal to prevent, detect, and respond to security incidents. This paper synthesizes insights from research on challenges related to employee information security practices and measures to address them. The challenges identified are associated to idiosyncratic aspects of communities and individuals within organizations (culture and personal characteristics) and to systemic aspects of organizations (procedural and structural arrangements). The measures identified aim to enhance systemic capabilities and to adapt security mechanisms to the idiosyncratic characteristics and are categorized as: (a) measures of training and awareness, (b) measures of organizational support, (c) measures of rewards and penalties. Further research is needed to explore the dynamics related to how challenges emerge, develop, and get addressed over time and also, to explore the interplay between systemic and idiosyncratic aspects. Additionally, research is needed on the role of security managers and how it can be reconfigured to suit flatter organizations.

Keywords: Information Security, Employees, Security Practices, Organizational Security Culture, Information Security Policies, Security Threats, Security Measures

INTRODUCTION

Information security is becoming a key concern for contemporary organizations as information systems are now ingrained in all aspects of operations and service provision. Organizations have to ensure that sensitive information is not accessed or modified by unauthorized persons and that is only available to employees entitled access rights (Ashenden & Sasse, 2013). Employee information security practices are pivotal for preventing, detecting, and responding to security incidents (Adele & Kulesa, 2016; McIlwraith, 2016; Wall, Lowry, & Barlow, 2016). Security issues originating from employee practices remain a persistent problem (Johnston, Warkentin, McBride, & Carter, 2016). Actually, internal threat is the most significant factor in the failure of IT security and employees are the top source of security incidents (Loft, He, Janicke, & Wagner, 2019; Price Waterhouse Coopers, 2017). In light of growing operational risks and increasingly demanding regulations (for instance, the Privacy Rule of Health Insurance Portability and Accountability Act -HIPAA, the Payment Card Industry Data Security Standard -PCI DSS, the European Union General Data Protection Regulation -GDPR), efforts towards information security are intensified and a growing body of research investigates employee security practices. This paper provides a comprehensive overview of extant research in this area charting findings, consolidating them in a classification framework and identifying key topics for future research.

The findings presented are based on a systematic literature review guided by the following research questions: (1) *What challenges related to employee information security practices have been identified in previous empirical research? (2) How are the challenges addressed in practice?*

The remainder of the paper is organized as follows. First, the review method is described. Then, the results are presented. Finally, the discussion and conclusion sections provide a synthesis and assessment of the results suggesting a concise classification framework and further research areas.

RESEARCH METHOD

The literature review is conceptual and provides a synthesis and assessment of prior research identifying research gaps and areas for future research (Ortiz de Guinea & Paré, 2017, Schryen et al. 2015). To ensure the relevance of selected literature, specific keywords along with a set of inclusion/exclusion criteria were used. The review includes research published during the last 10 years (from 2009 up to 2018). The process was guided by the guidelines suggested by Kitchenham that include three phases: (1) planning (e.g., identifying the need for a literature review, developing a procedure for conducting the review), (2) implementing (identifying previous research, selecting the main studies, undertaking quality assurance of the studies, collecting, synthesizing the studies), and (3) reporting and assessing the results (Kitchenham, 2004; 2009). The literature search was performed in Scopus and was confined to peer reviewed primary studies (not literature reviews) that include empirical data (not solely conceptual papers). The search strings used consist of term combinations linked to the research questions together with their synonyms (Table 1). The operators "AND" and "OR" were used to ensure a well-targeted and comprehensive search. Additionally, the wildcard character "*" was used to include variants of the keywords.

Table 1. Inclusion and exclusion criteria and search query

Inclusion criteria	Peer-reviewed, English, published in 2009 or later, empirical studies
Exclusion criteria	Exclude literature review studies, exclude studies on specific themes not related to the research questions (e.g., research on cryptography, security in mobile applications, RFID).
Search query	PART A: “information security policy” OR “data security policy” OR “information security awareness” OR “data security awareness” OR “information privacy policy” OR “data privacy policy” AND PART B: compliance OR conformance OR attitude* OR culture AND PART C: employee* OR person* OR human resources OR user*

To increase the relevance of the literature and to confine the set of papers to be reviewed to a manageable set, the exclusion and inclusion criteria presented in Table 1 were applied. Specifically, prior literature review studies and conceptual papers were excluded because the intention was to analyze the findings of original empirical research. Furthermore, since the study is oriented to security practices, studies that relate to special technical issues, such as cryptography, security in mobile applications, and radio-frequency-identification (RFID) were excluded. The initial set of studies identified includes 75 articles. This initial set was filtered by reading all the abstracts leading to 33 articles. As a final step, the full papers were read, resulting in a final list of 27 articles for further analysis.

The selected articles were coded and synthesized following a concept-centric logic (Webster & Watson, 2002). The data analysis was specifically focused on challenges and measures related to employee information security practices. The first step was to identify and list key concepts while reading each article. After completing this step, all the identified concepts were evaluated, consolidated and refined. Hence, the concepts emerged inductively from the literature. The articles and concepts were cross-analyzed to ensure consistency and comprehensiveness. The final set of concepts was used for developing a concept matrix that presents the associations between the articles and the concepts (Table 2). The development of the concept matrix was instrumental for bringing up insights from published research. In the next section, we present the analysis results.

RESULTS

The overview of the findings is presented in the concept matrix (Table 2) and explained in the paragraphs that follow. The different types of challenges related to employee information security practices are presented first, followed by the measures suggested in the literature.

Table 2. Concept Matrix

	Security Challenges				Measures to address Security Challenges		
	Procedural Arrangements	**Personal Characteristics**	**Organizational Culture**	**Structural Arrangements**	**Organizational support**	**Training - awareness**	**Rewards-penalties**
Alshare, et al. 2018		x	x		x		x
Ashenden & Sasse, 2013			x	x	x		
Bulgurcu et al. 2010		x			x	x	x
Chen et al. 2018	x		x			x	x
Chen et al. 2012		x				x	x
Da Veiga 2016	x		x		x		
Da Veiga & Eloff, 2010	x	x	x	x	x	x	
Da Veiga & Martins, 2017			x		x	x	
Eminağaoğlu et al. 2009	x				x	x	
Furnell & Thomson, 2009			x		x	x	
Guo et al. 2011		x					x
Hagen et al. 2011			x		x	x	
Hagen & Albrechtsen, 2009			x		x	x	
Herath & Rao, 2009		x			x		x
Hsu et al. 2015		x	x				
Karlsson et al. 2017	x	x			x		
Kolkowska et al. 2017	x	x				x	
Kolkowska & Dhillon, 2013				x	x		
McCormac et al. 2017		x			x	x	
Öğütçü et al. 2016		x			x		
Renaud, 2012	x			x	x	x	
Rocha Flores et al. 2016		x	x	x	x	x	
Safa et al. 2016		x	x				x
Siponen et al. 2014	x					x	x
Tsohou et al. 2012				x		x	
Tsohou et al. 2015		x	x	x		x	
Vance et al. 2012		x	x			x	

Challenges related to Information Security Practices in Organizations

In total, four key types of challenges were identified. Two of the four types are associated to the particularities of the communities and individuals within each organization. These challenges are rooted to the personal characteristics and attitudes of the employees and their organizational culture. They reflect the particular ways of behaving and thinking within an organization, and hence we label them as "idiosyncratic". Additionally, two more types of challenges were identified. These are associated to organizational arrangements at the procedural and structural level. They reflect the way the organization as a whole addresses security in terms of formal policies/rules and roles and hence we label them as "systemic".

Personal Characteristics and Security Attitudes

Several studies focus on personal characteristics that influence compliance or non-compliance (Hsu et al., 2015; Karlsson, Hedström, & Goldkuhl, 2017). Individual stances are related to several characteristics, such as age, marital status, education, emotional frames, values, and basic background. For instance, many employees tend to value job performance more highly than adherence to security rules (Guo, Yuan, Archer, & Connelly, 2011). Furthermore, prior research has shown that some employees may violate information security policies because security is not a personal priority for them and that responsibility is negatively correlated with violations of information security (Alshare, Lane, & Lane, 2018). Information security attitudes among employees are therefore important to understand because they influence security practices (Hsu et al., 2015). Individual and personal factors can affect the conformance and non-conformance to security standards and rules. McCormac and colleagues (2017) analyzed individual differences in terms of information security, examining demographics and different risk-taking behaviors. Bulgurcu and colleagues (2010) studied individual rationalization factors that support employees

in following the security rules of an organization. An illustration of personal differences is provided by Da Veiga and colleagues (2010) who discuss two opposing types of personalities (A and B) and their behavior in terms of information security. Type A employees work fast and tend to show how competent they are in terms of efficiency but often make poor decisions because they work at a fast pace. Personality B focuses on quality and is never concerned about time pressure. Type A employees often do not invest time to create strong passwords and choose to share passwords instead of waiting for access privileges. Type B employees often thinks twice before they do something and tend to use stronger passwords.

Organizational Culture

Having a strong organizational security culture is negatively correlated with information security violations (Alshare et al., 2018). Prior research has pointed to the difficulties of developing such a culture because of different understandings about security issues among organizational groups (Ashenden & Sasse, 2013; Furnell & Thomson, 2009; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015). When an organization has a poor security culture, serious security breaches can occur because employees easily break the rules and make the company vulnerable to attacks. Examples of a poor security culture include writing down passwords or giving away account information on request. Challenges in security culture can be linked to neglected security training (X. Chen, Chen, & Wu, 2018). In organizations that lack a security culture, employees can easily be victims of manipulation, for instance, opening e-mails that contain malicious software (Da Veiga, 2016; Da Veiga & Eloff, 2010; Furnell & Thomson, 2009; Hagen & Albrechtsen, 2009; Hagen, Albrechtsen, & Johnsen, 2011; Rocha Flores & Ekstedt, 2016; Safa, Von Solms, & Furnell, 2016; Vance, Siponen, & Pahnila, 2012). Da Veiga and Martins (2017), found that several unhealthy subcultures

may exist in parallel. Interestingly, in the case they studied, the management of the organization was not able to identify them.

Procedural Arrangements

Employee practices are shaped by information security policies (ISP) that contain rules and adopted standards. ISPs that are opaquely written or difficult to access may not be read by employees. Employees who have not read the rules are less receptive to introducing information security in everyday practices and have less understanding of what they have to do to protect their organization´s business resources (Da Veiga, 2016). It is not uncommon to find companies that only develop high level ISP documents lacking practical guidelines (Da Veiga & Eloff, 2010; Eminağaoğlu, Uçar, & Eren, 2009). Employees that do not have a good understanding of policies may develop risky behavior such as sharing passwords or using passwords that are easy to guess. The design of ISPs, and the formulation of procedures and rules can be challenging in practice and employees may find that the rules are impossible to follow (Karlsson et al., 2017; Renaud, 2012; Siponen, Mahmood, & Pahnila, 2014) leading to increased security incidents and ISP non-compliance (Kolkowska, Karlsson, & Hedström, 2017).

Structural Arrangements

Different security roles may exist within organizational structures, for instance, the role of the information security officer or of the chief information security officer (CISO). Traditionally, these roles had significant power in hierarchical organizations. This situation changes when organizations become flatter in structure, and this power becomes more difficult to maintain (Ashenden & Sasse, 2013). Security is difficult to convert into business value, and CISOs might meet challenges in delivering the required security measures. For example, an organization's overall strategy often includes different efficiency and productivity principles, and it is common

for employees to be rewarded in terms of how quickly and efficiently they work. Security may add obstacles and delays. Consequently, security demands are not always positively received within organizations and security managers may encounter problems communicating requirements.

Measures to address the challenges improving information security practices

Three major categories of measures to improve information security practices were identified in the literature: (a) measures related to training and awareness, (b) measures related to organizational support, (c) measures related to rewards and penalties. These measures aim to enhance systemic capabilities and to adapt security mechanisms to the idiosyncratic characteristics of organizations.

Training and awareness

Training and awareness campaigns were suggested in most of the papers in this literature review. High levels of information security awareness can positively affect employee attitudes towards information security (Bulgurcu et al., 2010). Organizations can work towards ensuring the right mindset and making certain that people endorse robust security routines (Furnell & Thomson, 2009; Hsu et al., 2015). Awareness, motivation and capability are important behavior drivers that can influence an employee's intention to comply with security policies (X. Chen et al., 2018). Furthermore, it is crucial to develop ethical awareness to enhance moral security standards (Y. Chen et al., 2012).

In their case study, Eminağaoğlu and colleagues (2009) show that by participating in security courses and continuous security campaigns, employees start to use stronger passwords. It is insufficient to just create an intranet page with all security procedures expecting that employees will remember the rules. Security courses are important for improving the security awareness of the organization. E-learning programs for security can make employees take responsibility for

their own learning processes (Hagen & Albrechtsen, 2009). Implementing e-learning initiatives can contribute to the improvement of the security culture (Hagen et al., 2011). By combining courses with hands-on assignments, a change in security behavior may be achieved (Rocha Flores & Ekstedt, 2016). Organizations should ensure that employees are provided with the time needed to gain knowledge about security. The training should be separate from everyday tasks, and employees may be offered the opportunity to complete the course at their own pace. If employees have faith in their own abilities, their intention to follow information security processes will increase (Bulgurcu et al., 2010; Herath & Rao, 2009; Siponen et al., 2014; Vance et al., 2012).

The management can promote and support groups that show the greatest interest in information security, for example, by motivating them to persuade others to pay attention to security in the organization (Da Veiga & Martins, 2017). Employees need to be constantly reminded that it is important to follow security rules (Siponen et al., 2014). Regular e-mails can be sent with different security messages (Da Veiga, 2016; Eminağaoğlu et al., 2009; Hagen et al., 2011), or security posters and brochures can be produced for distribution across the workplace to maintain awareness (Da Veiga, 2016). Increasing information security awareness requires organizations to focus on multiple areas simultaneously. Several researchers suggest that companies should use a framework when planning to increase security awareness (e.g. Da Veiga & Eloff, 2010; Tsohou et al., 2015).

Organizational support

Building and maintaining organizational support for information security entails consistent follow up and support of all decisions made regarding the implementation of security rules (Furnell & Thomson, 2009; Herath & Rao, 2009; Rocha Flores & Ekstedt, 2016; Siponen et al., 2014; Vance et al., 2012). Hagen and colleagues (2011), propose promoting a security culture by focusing on one group of employees at a time. This approach can create a positive effect that leads to more

people choosing to follow and adopt recommended security processes in their own work tasks. Herath and colleagues (2009) introduce measures that evaluate employees' security performance. Such measures may range from rounds in the employees' offices to see if they follow the security rules to evaluating logs. Controlling and measuring can show which part of the organization conforms to policies and rules and what part needs support to reach the desired level of security.

Organizations should ensure that a comprehensive and adequate set of information security components is in place. These components will help address different threats, for example, security breaches caused by employees or vulnerabilities of processes, or technical infrastructure. Information security rules can lead to significant changes. Such changes do not occur automatically and require mobilization and change in actions, consciousness, and values of employees (Kolkowska & Dhillon, 2013). Organizations need to ensure that employees' work is in line with the rules set (Da Veiga & Eloff, 2010; Kolkowska & Dhillon, 2013). It is important to avoid introducing security rules that are either impossible to follow or create ethical dilemmas; for this reason, Renaud (2012) suggests that organizations should involve employees in formulating security rules as this can improve practical relevance. Furthermore, employee involvement with developing information security measures is positively correlated to their implementation (Alshare et al. 2018). The security rules need to be simple, concise and understandable for the whole organization, and both managerial and employees' perspectives should be acknowledged when designing information security policies (Karlsson et al., 2017). Ashenden and Sasse (2013) propose that security managers should strive to create a two-way communication system to remove the "we and they" attitudes in the business. To achieve this objective, they must actively work to clarify their roles within the organization. It is important that security rules are readily available to

everyone in the organization (Da Veiga, 2016). Hagen et al. (2011) recommend implementing a technical system for storing and distributing the information security policies.

Rewards and Penalties

A reward may be either material or intangible compensation provided to employees that follow information security processes. In addition, penalties and rewards may be focused to enhancing motivation for compliance (X. Chen et al., 2018). Researchers have studied how different rewards or penalties increase or decrease employees' intention to follow security rules. Bulgurcu and colleagues (2010) suggest that rewards have a significant impact on employees' perception of the benefits of following the rules and that rewards can be effective motivators for adherence. However, Siponen and colleagues (2014) propose that rewards have no noticeable influence, but fear and perceived significance increase employees' intentions to follow security processes. They suggest that managers must communicate how serious security is for the business. Herath and colleagues (2009) discuss whether pressure and sanctions may compel employees to follow information security policies. Alshare and colleagues (2018) point to the need to not focus only on the severity of sanctions but also on their celerity or swiftness of application. Findings from a study conducted by Y. Chen and colleagues (2012) demonstrate that the severity and certainty of punishment as well as the significance of rewards, discourage employees from security policy violation. Rewards can be useful for organizations where sanctions did not work. Punishment may create a non-motivating atmosphere and the authors suggest a security enforcement system including a reward scheme that pays attention to moral standards and values. Overall, employees who know that they will be rewarded if they do something right or punished if they do something wrong show a higher motivation to follow the rules (Herath & Rao, 2009; Safa et al., 2016). However, the importance of high job performance is likely to outweigh the negative effect of

perceived sanctions. If security rules hinder the execution of work activities, the employees would rather aim for good job performance despite violating the security policy.

DISCUSSION

The literature review presented in this paper distills prior empirical research related to employee security practices covering both challenges and measures to address these challenges. For practitioners, the challenges and measures identified can serve as a starting point for formulating an effective information security approach. For researchers, the literature review can be a basis for further research and for conceptual development.

The review confirmed that there are persistent challenges that relate to weak employee security practices and non-secure employee behavior. These challenges are associated to idiosyncratic aspects of the communities within the organization and the individual employees (culture and personal characteristics) and to systemic aspects of organizations (procedural and structural arrangements). An overall graphical representation of the two dimensions is provided in Figure 1. As shown in this overall mapping, the organizational culture can create issues when there are entrenched unhealthy subcultures, heterogeneous understanding among employees and distanced management. Furthermore, personal characteristics including individual rationalization factors, age, education and prior experiences can contribute to security problems. Procedural arrangements that are incomprehensible or impractical or inaccessible can also impede security. Finally, structural arrangements related to misaligned rewards, job profiles that do not link to security and demoted positioning of CISOs also relate to security challenges.

The measures identified in the literature fall in three major categories: (a) measures related to training and awareness, (b) measures related to organizational support, (c) measures related to

rewards and penalties. The training and awareness measures proposed in the literature aim to address the idiosyncratic characteristics of organizations and their employees (by promoting approaches that are tailored to the educational background, experiences and risk-taking behaviors and by advocating self-paced programs) and to enhance their systemic capabilities (by introducing frameworks for analyzing and controlling training and awareness initiatives and by promoting continuity). Similarly, the measures that relate to organizational support not only aim to enhance systemic capabilities (by making information available through information security systems and assessing and improving measures in place) but also to address organizational idiosyncrasies (for instance, by involving employees in formulating rules, aiming to remove "we" and "they" attitude, focusing on one group of employees at a time).

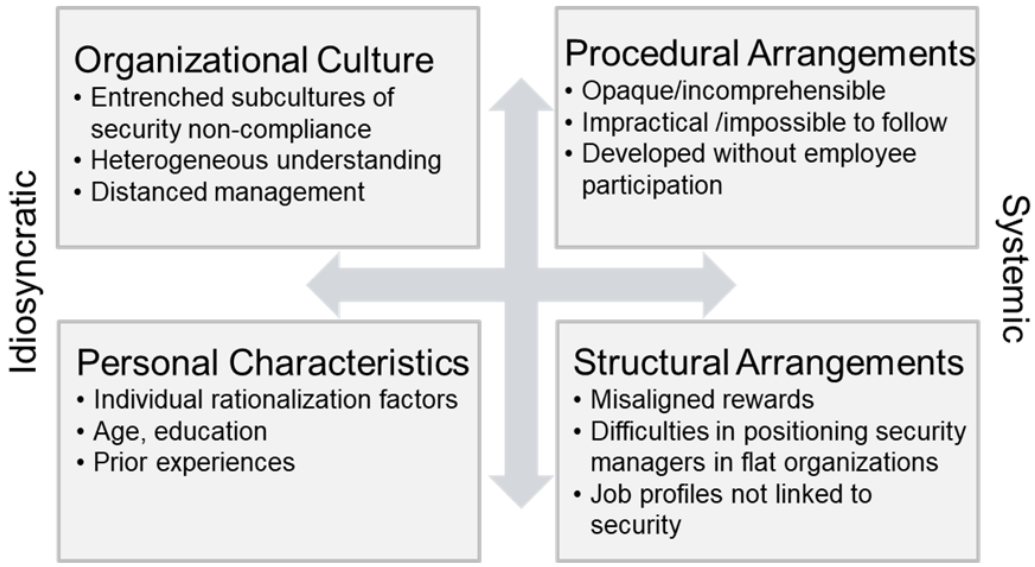

Figure 1. A framework synthesizing challenges for employee security practices

Regarding rewards and penalties, prior research is inconclusive. In some cases, rewards have no noticeable influence while sanctions seem to compel employees to follow information security

policies. Nevertheless, punishment may create a non-motivating atmosphere. Overall, a comprehensive scheme of rewards and sanctions related to moral standards and values seems to be a good approach.

DIRECTIONS FOR FURTHER RESEARCH AND CONCLUSION

The assessment of the review results led to the identification of research gaps that warrant further research. Specifically, we identified the need for more longitudinal research focusing on how challenges emerge, develop, and get addressed over time. Further research is also needed to understand the interplay between systemic aspects (procedural and structural) and idiosyncratic aspects (organizational culture and personal characteristics of individuals). Additionally, the analysis of recently published research revealed the need to research how the role and the positioning of security managers can be reconfigured to suit flatter contemporary organizations.

The first further research direction relates to the observation that longitudinal research is scarce among the studies reviewed. Most of the papers analyzed bring insights related to a specific point in time. Hence, there are limited insights related to the evolution of challenges and related measures over time. For instance, awareness campaigns need to be sustained over prolonged periods of time to build and maintain a focus on security. If more studies were based on longitudinal data (as for instance in the studies of Hagen and colleagues (2009) and Hagen and colleagues (2011)), more insights related to temporal aspects would have been available. Further research needs to be pursued taking a *process study approach* focusing on how and why security challenges emerge, develop, and get addressed over time. Process studies take the timeframe into account by identifying and explaining patterns in organizational phenomena.

Furthermore, the literature review identified the need for further research to investigate how the *role and the positioning of security managers* should be defined within contemporary organizations. Prior empirical research identified a tendency towards the adoption of flatter organizational structures. This makes it more difficult to keep the role of security managers visible.

Further research is also needed to understand *the interplay between systemic aspects* (procedural and structural) and *idiosyncratic aspects* (cultural and related to individuals). For this aim, it would be interesting to develop a *survey* instrument covering the dimensions depicted in the framework shown in Figure 1 and collect requisite data from multiple organizations. The data can be used to detect and model the relationships between different systemic and idiosyncratic aspects that shape employee security practices. A better understanding of the interplay between procedural, structural, cultural and individual aspects can support the customization of measures for organizational support, training and awareness, rewards and penalties guiding employees towards compliance with security policies and procedures.

Effective information security requires appropriate technical solutions but also sound employee security practices during everyday work. It is therefore important to assess employee practices and introduce security initiatives that address challenges raising the overall security level. At the same time, it is important to counterbalance the stressful effects of information security requirements preventing security-related overload, complexity, and uncertainty (D'Arcy, Herath, & Shoss, 2014). To sustain a good security culture, organizations need to embed in everything they do tailored measures addressing the weaknesses and leveraging the strengths of their employees. This requires time and effort but can provide significant returns on the investment by lowering vulnerabilities. For most organizations, employees are the top source of security incidents;

improving employee practices is pivotal for improving information security and reducing operational risk.

REFERENCES

Adele, A., & Kulesa, P. (2016). The inside threat: Why employee behaviour and opinions impact cyber risk. Available from: https://www.willistowerswatson.com/en/insights/2016/05/inside-threat-why-employee-behavior-and-opinions-impact-cyber-risk

Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: a higher education case study. *Information & Computer Security*, *26*(1), 91-108.

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security, 39*, 396-405.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548.

Chen, X., Chen, L., & Wu, D. (2018). Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective. *Journal of Computer Information Systems, 58*(4), 312-324.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157-188.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(2), 285-318.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not Illustrated through an empirical study. *Information and Computer Security, 24*(2), 139-151.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207.

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security, 70*, 72-94.

Eminağaoğlu, M., Uçar, E., & Eren, S. (2009). The positive outcomes of information security awareness training in companies - A case study. *Information Security Technical Report, 14*(4), 223-229.

Furnell, S., & Thomson, K.-L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security, 2009*(2), 5-10.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203-236.

Hagen, J. M., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management and Computer Security, 17*(5), 388-407.

Hagen, J. M., Albrechtsen, E., & Johnsen, S. O. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security, 19*(3), 140-154.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research, 26*(2), 282-300.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems, 25*(3), 231-251.

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security, 67*, 267-279.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University, 33*(2004), 1-26.

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and Software Technology, 51*(1), 7-15.

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security, 33*, 3-11.

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. *The Journal of Strategic Information Systems, 26*(1), 39-57.

Loft, P., He, Y., Janicke, H., & Wagner, I. (2019). Dying of a hundred good symptoms: why good security can still fail-a literature review and analysis. *Enterprise Information Systems*, OnlineFirst: DOI: 10.1080/17517575.2019.1605000, 1-26.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior, 69*, 151-156.

McIlwraith, A. (2016). *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*: Routledge.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83-93

Ortiz de Guinea, A., & Paré, G. (2017). *What literature review type should I conduct?* In The Routledge Companion to Management Information Systems (pp. 73-82). Routledge.

Renaud, K. (2012). Blaming noncompliance is too convenient: What really causes information breaches? *IEEE Security and Privacy, 10*(3), 57-63.

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers and Security, 59*, 26-44.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

Schryen, G., Wagner, G., & Benlian, A. (2015). Theory of knowledge for literature reviews: an epistemological model, taxonomy and empirical analysis of IS literature. *Proceedings of the 36th International Conference on Information Systems (ICIS) 2015*, Fort Worth, TX.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. *Information Technology & People*, 25(3), 327-352.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems, 24*(1), 38-58.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3-4), 190-198.

Wall, J. D., Lowry, P. B., & Barlow, J. B. (2016). Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess. *Journal of the Association for Information Systems, 17*(1), 39–76.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii-xxiii.