Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2018 Proceedings

Mediterranean Conference on Information Systems (MCIS)

2018

Information Security Practices in Organizations: A Literature Review on Challenges and Related Measures

Frode Mathias Bekkevik
University of Agder, Norway, frodeb13@student.uia.no

Ole Reidar Holm
University of Agder, Norway, olerh16@student.uia.no

Polyxeni Vassilakopoulou
University of Agder, Norway, polyxenv@uia.no

Eli Hustad
University of Agder, Kristiansand, Norway, eli.hustad@uia.no

INFORMATION SECURITY PRACTICES IN ORGANIZATIONS: A LITERATURE REVIEW ON CHALLENGES AND RELATED MEASURES

Research full-length paper

Track Security and Privacy

Bekkevik, Frode Mathias, University of Agder, Norway, frodeb13@student.uia.no

Holm, Ole Reidar, University of Agder, Norway, olerh16@student.uia.no

Vassilakopoulou, Polyxeni, University of Agder, Norway, polyxenv@uia.no

Hustad, Eli, University of Agder, Norway, eli.hustad@uia.no

Abstract

This paper reports a systematic literature review that explores challenges related to information security practices in organizations and the ways these challenges are managed to avoid security breaches. We focused on empirical evidence from extant research studies and identified four general challenges related to: (1) security rules and procedures, (2) individual and personal risks, (3) culture and security awareness, and (4) organizational and power relations. To manage these risks, nine measures were prominent in the selected studies. Training and organizational collaboration across the hierarchical levels were widely used to enhance the security culture. In addition, awareness campaigns for the workforce, as well as continuously measuring and improving security initiatives were highly recommended. Our literature review points to the socio-technical aspects of information security. Although many organizations have both administrative and technical infrastructures in place, they must also think about employee attitudes, knowledge, and behavior. Information systems research towards this direction needs to be further developed. More qualitative studies are needed for exploring how to develop a culture of security awareness and for gaining insights on how security rules and training courses can become more appealing and accessible.

Keywords: Information security, culture and security awareness, security threats, security measures

1 Introduction

Contemporary organizations in our digital society use a lot of resources to protect sensitive information. Most enterprises have trade secrets concerning customers, contracts, internal procedures, and methods that they want to keep confidential or other information that they do not want to share to avoid losing competitive advantages. Information security is about ensuring that business-sensitive information is not accessed or modified by unauthorized persons and that the information is only available for the employees who are supposed to have access to it when needed (Ashenden et al. 2013).

Information security in organizations is an important and current topic that has evolved in line with digitization. Recently, media has paid attention to a series of data attacks against various businesses in Europe (Euronews 2018). Several reports point to employee behavior as a key threat creating security risks (Adele et al. 2016).

In 2003, Logan and colleagues conducted a case study on information security reporting from a company that was completely battered by malware. However, much of the damage could have been prevented if appropriate security attitudes were established among employees (Logan et al. 2003).

In a recent book on organizational security written by McIlwraith (2016), the focus on information security 'awareness' is highlighted as fundamental to handle security breaches. Working with this topic for a long time, the author is motivated by the problems large consultancy firms meet in practice, for example as stated in a global security report from Deloitte in 2005: "it is clear that many security breaches are the result of human error or negligence resulting from weak organizational practices". Furthermore, awareness is also highlighted in a later report: "People are part of the problem when it comes to information security, so they need to be part of the solution. Training and awareness may help organizations manage the risks from new technologies" (Deloitte 2013).

However, a different understanding of awareness is needed, and changes in human behavior and attitudes are required to handle breaches in an improved manner. Organizations need to develop a comprehensive approach that consider both the social and the technical dimensions: "Human error is often the root cause of problems in some of the most sophisticated technological implementations. This is why security awareness in your company is so critical" (Voss 2011, cited in McIlwraith 2016, p.5).

These recent reports on security risks as well as the abovementioned statements, motivates this research. There is a need to get an overview of extant research on information security practices and how security threats are tackled. In addition, it is crucial to get an overview of which topics future research should concentrate on with respect to information security.

Accordingly, in this paper we seek to get an overview of previous empirical studies focusing on information security practices in organizations to consolidate knowledge in the domain, identify possible research gaps and create a solid basis for future research. We conducted a systematic literature review guided by the following research questions: (1) *What challenges related to information security practices in organizations have been addressed in previous research?* (2) *How are the identified information security challenges managed in practice?*

The paper is organized as follows. First, we provide an overview of how the literature review was conducted. Second, we present the main results. Then we discuss our results and provide implications for future research. Finally, we make some concluding remarks.

2 Research Method

A systematic literature review allows researchers to obtain an overview of existing studies in a specific area, making it easy to identify gaps and to propose future research recommendations. In this literature study, we have utilized the guidelines suggested by Kitchenham (Kitchenham 2004; 2009). The guide-

lines include three phases: (1) planning (e.g., identifying the need for a literature search on organizational security risks, developing a procedure for conducting the study), (2) implementing (identifying previous research, selecting the main studies, undertaking quality assurance of the studies, collecting and monitoring the data, and synthesizing the data), and (3) reporting the results.

To ensure the quality and relevance of selected papers we used a set of inclusion and exclusion criteria (Table 1).

Inclusion criteria	Peer-reviewed, English, published in 2007 or later, primary keyword should be in the title of the paper, empirical studies
Exclusion criteria	Exclude literature review studies, exclude studies on specific themes not related to the research questions (e.g., technological aspects such as cryptography, security in mobile applications, RFID).

Table 1. Inclusion and exclusion criteria

We performed a search in four different databases: EBSCO, ORIA, Scopus, and Web of Science. The search strings used consist of relevant combinations of the main theme of information security, together with various synonyms and secondary search terms directly linked to the research questions. The primary search term (A) was "information security" and its associated terminology. We also used secondary search terms (B) and tertiary keywords (C) to include human factor aspects of information security (see Table 2).

Search Category	Keywords (Search String)
A1	information security awareness
A2	information security policy, data security policy
A3	information privacy policy, data privacy policy
B	Compliance, conformance, attitude*, culture
C	employe*, person*, human resources, user*

Table 2. Overview of keywords in different search categories

We chose to include several different keywords and search categories because information security is ambiguously defined in the literature, and information systems research contains socio-technical aspects. For example, social factors comprise several themes, such as culture, training, and practices. Furthermore, we used "AND" and "OR" operators to refine the search. The "AND" operator ensured the presence of the primary search term (A), the secondary search word (B), and the tertiary keyword (C). The "OR" operator was used to include synonyms of selected keywords and to create more complex search strings. We also used the wildcard character "*" to include variants of the same keyword. For example, "employe*" would include words such as employed, employee, employees, and employer.

All search hits were added to the EndNote citation management application. Using the application, we categorized the sources based on combinations of the keywords. For example, the primary search word (A) and the secondary search word (B) combinations were assigned to separate categories of hits from the four databases we used (EBSCO, ORIA, Scopus, and Web of Science). Our reason for doing this was to compare relevant hits from the various databases. We exported the lists of papers identified through all search queries and removed duplicates.

To increase the relevance of the literature and to confine the set of papers to be reviewed to a manageable set, we performed a quality assessment of the individual articles identified. For the quality assessment we evaluated each article's relevance (importance) in relation to our study's main theme. The exclusion and inclusion criteria presented in table 1 were used at this stage. We excluded former literature review

studies because our intention was to analyze organizational security risks based on empirical research. Because of our socio-technical focus, we excluded studies that were related to special technological issues, such as cryptography, security in mobile applications, and radio-frequency-identification (RFID).

We continued by reading all the abstracts and ended up with 33 articles that met our inclusion criteria. We then read the full papers and selected the most relevant ones based on the whole content and ended up with 20 articles for further analysis (see Appendix 1). We used an article matrix to collect and structure the data from each article. The matrix was continuously changed; the categories, concepts, and topics were added and/or removed throughout the process.

First, we conducted a meta-analysis of the findings to identify the research methods and the contexts of the studies. Second, we classified the different concepts that consisted of various organizational security risks and actions to address these risks/challenges. We followed Webster and colleagues (2002) suggestion that a literature review is concept-oriented rather than author-directed.

3 Main results of the literature review

3.1 Overview of key meta-data

We found that the majority of the selected papers applied quantitative research methods, most frequently based on surveys. Only one-quarter of the papers used qualitative methods, including case studies with interviews, observations, and document collections. The research contexts of the studies were mainly European countries; only a few studies were conducted outside Europe (Asia, Australia, the US, and Africa). The participants in the studies had the roles of manager, employee, external stakeholder, and expert/researcher. Finally, more studies were conducted in the public sector compared with the private sector.

3.2 Key concepts and related topics

The analysis of the core findings concentrated on two main categories: (1) identified challenges related to information security practices in organizations and (2) initiatives to address the information security challenges.

In the following paragraphs we present the content of the concept matrix developed (see Figure 1). First, the different types of challenges identified are presented, followed by the solutions suggested in the literature.

3.2.1 Identified challenges related to information security practices in organizations

In total, four key types of challenges were identified. Specifically, the challenges relate to:

- security rules and procedures,
- individual and personal risks,
- culture and security awareness, and
- organizational and power relations.

These are outlined in the following paragraphs.

Security rules and procedures; Information security rules and procedures are established to protect the organization's resources. The information systems policy (ISP) contains adopted standards and rules that guide employees on what to do to protect their organization's business resources. One of the issues related to security rules and procedures is that it is not uncommon to find employees who have neither read the company's security rules nor know how to find them. Employees who have not read the rules

are also less receptive to introducing information technology (IT) security into their work and have less understanding of the rules (Da Veiga 2016). With limited awareness of security rules and procedures employees may develop risky behaviors such as sharing their passwords with one another or using simple passwords that are easy to guess. In some cases, companies may not have in place any formal rules that explain and operationalize IT security policies (Da Veiga et al. 2010; Eminağaoğlu et al. 2009). There are also cases where the rules themselves are the problems. Employees may find that the rules are impossible to follow, and sometimes, they are written in an incomprehensible manner (Renaud 2012; Siponen et al. 2014).

Individual and personal risks; Employees are often regarded as the weakest link in business information security (Bulgurcu et al. 2010). Individual and personal factors can affect the conformance to security standards and rules. Employees who choose to follow the rules and the procedures help create more robust information security in the business. Bulgurcu and colleagues (2010) studied various individual rationalization factors that might support the employees in following the security rules of an organization. For example, when the employees have a positive attitude toward the security rules in their workplace, their intention to follow these rules is high.

However, attitude and behavior do not characterize all the influencing factors. Various individual and personal factors comprise other characteristics, such as age, marital status, education, emotional frameworks, values, and basic background. In a workplace, several types of people and personalities are present. There may be major differences between these people and their intention to follow security rules. Da Veiga and colleagues (2010) discuss two opposing personalities (A and B). Personality A may be concerned with quantity over quality. Type A employees work fast and illustrate how competent they are in terms of work hours 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 have limited time to create strong passwords and choose to share passwords instead of waiting for access privileges. Type B employees often think twice before they do something and tend to use stronger passwords.

Main concepts and related topics / Author		Ashenden & Sasse (2013)	Bulgurcu, Cavusoglu & Benbasat (2010)	Da Veiga (2016)	Da Veiga & Eloff (2010)	Da Veiga & Martins (2017)	Eminağaoğlu, Uçar & Eren (2009)	Furnell & Thomson (2009)	Hagen, Albrechtsen & Johnsen (2011)	Hagen & Albrechtsen (2009)	Herath & Rao (2009)	Kolkowska & Dhillon (2012)	McCormac et al. (2017)	Ogutcu, Tastik & Chouseinoglou (2016)	Renaud (2012)	Rocha Flores & Ekstedt (2016)	Safa, Von Solms & Furnell (2016)	Siponen, Mahmood & Pahnila (2014)	Tsohou et al. (2012)	Tsohou et al. (2015)	Vance, Siponen & Pahnila (2012)
Security challenges	Definition of security rules and procedures			x	x		x								x			x			
	Individual and personal risks		x		x						x		x	x		x	x			x	x
	Culture and security awareness	x		x	x	x		x	x	x						x	x			x	x
	Organizational and power relations	x			x							x			x	x			x	x	
Initiatives to address security challenges	Organizational support and cooperation	x						x	x	x	x	x		x	x	x	x	x	x	x	x
	Training and awareness campaigns		x	x	x		x	x	x	x		x	x	x		x	x	x	x	x	x
	Rewards and penalties		x								x						x	x			
	Set of information security components		x	x	x	x		x	x		x	x			x			x			x
	A framework to increase security awareness				x			x	x	x					x				x	x	
	Implementation of an ISS								x						x						
	Ongoing awareness campaigns					x	x	x	x									x	x		x
	Checking, measuring, and improving security initiatives						x				x							x	x		
	Individual courses and training programs												x			x				x	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Figure 1. Concept matrix and topics of selected papers from the literature review

Culture and security awareness; Information security is perceived as a specific aspect of organizational culture. Not all employees understand organizational security as part of their daily work practice. Security managers fail to implement a security culture in the organization because of different understandings about security issues among organizational groups, as well as the distance between the management and the hierarchical levels (Ashenden et al. 2013; Furnell et al. 2009; Tsohou et al. 2015).

If an organization has a poor security culture, serious security breaches can occur because employees easily break the information security rules without knowing them and make the company vulnerable to attacks. Examples of a poor security culture are not locking the PC when leaving the office, writing down passwords, or giving away account information on request. These situations typically occur when security training is neglected, and the employees do not know the company's IT security rules. They can therefore be easy victims of social manipulation, for example, by opening e-mails that contain malicious software (Da Veiga 2016; Da Veiga et al. 2010; Furnell et al. 2009; Hagen et al. 2009; Hagen et al. 2011; Rocha Flores et al. 2016; Safa et al. 2016; Vance et al. 2012). Da Veiga and Martins (2017), found in their study that several unhealthy subcultures may exist in parallel. Interestingly, in the case studied, the management of the organization was not able to identify them.

Organizational and power relations; Information security goals must be aligned with formal business processes to deliver beneficial results. Although there are different information security standards for linking business processes and security goals, this can be a complex undertaking. Different security roles exist in organizations, 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 et al. 2013).

Security is difficult to convert into business value, and CISOs might meet challenges delivering the required security measures. For example, an organization's overall strategy often starts with different efficiency and productivity principles, and it is common for its employees to be rewarded in terms of how quickly and efficiently they work. Thus, an extra security layer may also add obstacles. Consequently, security demands are not always positively received within an organization, which causes the security managers to encounter problems communicating security requirements.

3.2.2 Initiatives to address the challenges

In total, nine different types of initiatives were identified for addressing the challenges related to information security practices in organizations:

- organizational support and cooperation;
- training and awareness campaigns;
- rewards or penalties;
- comprehensive and adequate sets of information security components;
- frameworks to increase security awareness;
- implementation of information security systems (ISS);
- ongoing awareness campaigns;
- assessing, measuring, and improving security initiatives; and
- individual courses and training programs.

These are explained in the following paragraphs.

Organizational support and cooperation; It is not easy for management to build and maintain its organizational culture; it is necessary to consistently follow up and support the decisions made regarding

implementation of security rules (Furnell et al. 2009; Herath et al. 2009; Rocha Flores et al. 2016; Siponen et al. 2014; Vance et al. 2012). Hagen et al. (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 positions in their own work tasks. The management should also encourage employees to participate in information security courses and support employees in obtaining the required security knowledge (Hagen et al. 2009).

It is also important to consider that an information security rule can lead to strategic changes. Such strategic changes do not occur automatically, requiring mobilization and change in actions, consciousness, and values of the workers (Kolkowska et al. 2012). To solve the problem of security rules that are either impossible to follow or create ethical dilemmas, Renaud (2012) suggests that the organization should involve employees in formulating these rules. In this way, employees feel acknowledged, which can strengthen the company's information security. Moreover, Ashenden and Sasse (2013) state that security managers have difficulties in communicating with their employees. The authors propose that CISOs should strive to create a two-way communication system to remove the "we and they" attitudes in the business. To achieve this objective, the CISOs must actively work to clarify their roles within the organization.

Training and awareness campaigns are the actions suggested in most of the selected studies in this literature review. Ensuring high information security awareness (ISA) in the organization can directly and indirectly change employee attitudes towards information security (Bulgurcu et al. 2010). In practice, this is about ensuring the right mindset and making certain that people work for robust security routines instead of against them (Furnell et al. 2009). 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.

Organizations should ensure that employees are provided with the time needed to be involved to gain better 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. To derive the most benefits from security training, organizations should tailor the program so that all employees understand its content and importance. Security must not be regarded as a burden but part of the daily work routine. If employees have faith in their own abilities (self-efficacy), their intention to follow information security processes will increase (Bulgurcu et al. 2010; Herath et al. 2009; Siponen et al. 2014; Vance et al. 2012).

Rewards and penalties; A reward may be either material or intangible compensation that an organization provides to its employees for following information security processes. 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.

On the other hand, Herath and colleagues (2009) discuss whether pressure and sanctions may compel employees to follow the ISP. They find that different internal and external motivation factors have effects. If an employee understands that it will come to light that the security rules are broken, the intention to follow rules increases. However, Siponen and colleagues (2014) propose that rewards have no noticeable influence, they suggest that fear and perceived significance increase employees' intentions to follow security processes. They suggest that managers must communicate how serious security is for the business.

Comprehensive and adequate set of information security components; Information security rules and procedures are critical success factors for establishing a strong information security culture. These rules can guide employees' attitudes in the right direction. It is therefore important that they are readily available to everyone in the organization (Da Veiga 2016).

Organizations should ensure that a comprehensive and adequate set of information security components is implemented. These components will help address different threats, for example, security breaches

caused by employees or vulnerabilities of processes, or technical infrastructure. The organization should also warrant that employees' work is in line with the rules set (Da Veiga et al. 2010; Kolkowska et al. 2012).

A framework to increase security awareness; 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 et al. 2010; Tsohou et al. 2015). The literature provides several frameworks and methods that seek to solve the threats generated by the employees. For example, Da Veiga and colleagues (2010) propose an extensive framework for creating an organizational security culture. The framework explains how information security components affect security behavior and help create a culture of security. Tsohou et al. (2015) argue that information security awareness processes are associated with the interrelated changes that occur at the organizational, technical, and individual levels. They introduce a framework to analyze and control the changes that occur when implementing an information security awareness program.

Implementation of an information security system (ISS); Hagen et al. (2011) recommend implementing a technical system for storing and distributing the information security policies. Additionally, they propose introducing e-learning initiatives encompassing every section of the security rules of the organization. Such initiatives can offer employees good learning experiences in information security. Moreover, they will have a common platform for giving and receiving feedback and finding all policies in one place, and they will be able to review previous security courses.

Renaud (2012) proposes the introduction of a password management system. Such a system can generate secure passwords for all the other information systems in use, so employees only need to remember one password at a time.

Ongoing awareness campaigns; According to Da Veiga (2016), employees who have read the security regulations will acquire higher security competencies compared with their counterparts who have not come across the regulations. This assertion is partly true. In many cases, security awareness is given low priority compared to other IT training courses (Furnell et al. 2009). It is insufficient to just create a simple intranet page with all security procedures expecting that employees will remember the rules. Security training courses work only in the short term; however, they are important for improving the security awareness of the organization.

Managers must constantly remind employees 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 some security posters and brochures can be produced for distribution across the workplace to maintain awareness (Da Veiga 2016).

E-learning programs for security can make employees take responsibility for their own learning processes (Hagen et al. 2009). Implementing an extensive e-learning initiative can contribute to the improvement of the security culture (Hagen et al. 2011). The management can promote and support groups or subcultures that shows the greatest interest in information security, for example, by motivating them to persuade others to pay attention to security in the organization (Da Veiga et al. 2017).

Assessing, measuring, and improving security initiatives; Eminağaoğlu and colleagues (2009) discuss password complexity, that was measured among employees over a 12-month period. Implementing password complexity, can create higher quality passwords and higher security awareness among the employees. Controlling, measuring, and improving security measures can show employees which part of the organization conforms to the policies and rules and what aspects need more support to reach the desired level of security.

Herath and colleagues (2009) introduce measures that evaluate employees' security performance. Such measures may include anything, ranging from rounds in the employees' offices to see if they follow the

security rules to evaluating the logs. Employees who see the likelihood of negative consequences for violating the information security rules are more probable to follow the rules.

Individual courses and training programs; McCormac and colleagues (2017) analyze individual differences in terms of information security, examining demographic, personal, and risk-taking behaviors. By combining courses with hands-on assignments, a change in security behavior may be achieved (Rocha Flores et al. 2016).

4 Discussion

The security topics that are foregrounded in the selected studies include organizational support and collaboration regarding security issues, security training, and awareness campaigns. Training and collaboration are recommended combinations to increase employee awareness and expertise in information security. For instance, employees with high levels of information security awareness create a safer workplace because they do not make high-risk decisions regarding information security. Unfortunately, many organizations fail to maintain a high level of information security awareness over a long term. A continuous program that focuses on information security is required to ensure that employees will be reminded of the rules.

An interesting finding is that only seven articles from the literature synthesis discuss ongoing awareness campaigns as important actions to maintain the focus on security. Repeated security campaigns and training are described as among the most important measures for ensuring continuous knowledge development on security. Organizations tend to spend a lot of resources on security initiatives that may be wasted if they do not have an ongoing character.

The lack of emphasis on ongoing security measures in the literature reviewed may be attributed to the methodological approaches of the articles. Most of the articles are quantitative and/or measure effects at only one point in time. If more studies had collected longitudinal data to ensure data from multiple points in time (as for instance in the studies Hagen and colleagues (2009) and Hagen and colleagues (2011)), measures such as improvement programs for security initiatives, ongoing awareness campaigns, and individual training programs would receive more attention. These are types of measures that may prove effective over a longer period of time. Furthermore, to achieve the best possible outcomes of new security initiatives, organizational support across hierarchical levels is required.

Rewards and sanctions have been widely discussed in the research literature. Rewards will not directly affect employee compliance to security rules but may serve as effective motivational factors (Bulgurcu et al. 2010). 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 security rules (Herath et al. 2009; Safa et al. 2016). Nevertheless, this claim is not supported by Siponen and colleagues (2014), who find no connection between rewards and employees' intentions of following the security rules. Siponen and colleagues (2014), argue that rewards do not work.

This literature review has some implications for practice. First, management teams must remind employees that information security breaches can occur and that such breaches can have major consequences for the organization. The senior management should be involved in designing and distributing these messages. Regular meetings and security courses should be organized to remind employees of the importance of following security standards and rules. The security rules need to be simple, concise and understandable for the whole organization. Employees must have access to security training and practical training all the time to build the confidence they need to follow security rules without assistance.

Further research is needed to investigate how the role and the mandate of the security manager should be defined to prevent this role from becoming under-prioritized. We observed a tendency for organizations to adopt flatter organizational structures. This makes it more difficult to keep the role of security managers visible. Additionally, it would be interesting to study how awareness campaigns and security training can work on a long-term basis.

5 Conclusion

Our study identified challenges related to information security practices found in previous empirical studies, and how these challenges are addressed through different security initiatives. Challenges associated with culture and security awareness are most prevalent in the research literature while training and organizational collaboration across hierarchical levels are the two most widely discussed types of initiatives.

Effective information security requires appropriate technical solutions but also sound information security practices during everyday work. Although many organizations have both administrative and technical infrastructures in place, they must also think about employee attitudes, knowledge, and behavior. It is therefore important to assess, measure, and improve security initiatives to reveal areas that need more support to reach the desired level of security. To sustain a good security culture, organizations must create ongoing security campaigns to help employees remember security rules. Such campaigns can include promotional material such as posters, e-mails, e-learning courses, as well as managers' direct communication with employees.

References

Adele, A., and Kulesa, P. 2016. "The inside threat: Why employee behaviour and opinions impact cyper risk," Willis Towers Watson, available from: https://www.willistowerswatson.com/en/insights/2016/05/inside-threat-why-employee-behavior-and-opinions-impact-cyber-risk.

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

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

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), pp 139-151.

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

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

Deloitte 2013. "Information security in a world without boundaries," https://www2.deloitte.com/cy/en/pages/technology-media-and-telecommunications/articles/2013-tmt-global-securitystudy.html.

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

Euronews 2018. "Cyber Attacks," a. f. http://www.euronews.com/tag/cyber-attacks (ed.).

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

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

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

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

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

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

Kolkowska, E., and Dhillon, G. 2012. "Organizational power and information security rule compliance," *Computers & Security*).

Logan, P. Y., and Logan, S. W. 2003. "Bitten by a bug: a case study in malware infection," *Journal of Information Systems Education* (14:3), p 301.

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

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

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

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

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

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

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

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

Webster, J., and Watson, R. T. 2002. "Analyzing the past to prepare for the future: Writing a literature review," *MIS quarterly*), pp xiii-xxiii.

#	Author (s)	Title of paper	Year	Publication outlet
1	Ashenden & Sasse	CISOs and organizational culture: Their own worst enemy?	2013	Computers & Security
2	Bulgurcu, Cavusoglu & Benbasat	Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness	2010	MIS Quarterly
3	Da Veiga	Comparing the information security culture of employees who had read the information security policy and those who had not Illustrated through an empirical study	2016	Information and Computer Security
4	Da Veiga & Eloff	A framework and assessment instrument for information security culture	2010	Computers & Security
5	Da Veiga & Martins	Defining and identifying dominant information security cultures and subcultures	2017	Computers & Security
6	Eminağaoğlu, Uçar & Eren	The positive outcomes of information security awareness training in companies - A case study	2009	Information Security Technical Report
7	Furnell & Thomson	From culture to disobedience: Recognizing the varying user acceptance of IT security	2009	Computer Fraud & Security
8	Hagen, Albrechtsen & Johnsen	The long-term effects of information security e-learning on organizational learning	2011	Information Management & Computer Security
9	Hagen & Albrechtsen	Effects on employees' information security abilities by e-learning	2009	Information Management & Computer Security
10	Herath & Rao	Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness	2009	Decision Support Systems
11	Kolkowska & Dhillon	Organizational power and information security rule compliance	2012	Computers & Security
12	McCormac et al.	Individual differences and Information Security Awareness	2017	Computers in Human Behavior
13	Ogutcu, Tastik & Chouseinoglou	Analysis of personal information security behavior and awareness	2016	Computers & Security
14	Renaud	Blaming noncompliance is too convenient: What really causes information breaches?	2012	IEEE Security and Privacy
15	Rocha Flores & Ekstedt	Shaping intention to resist social engineering through transformational leadership, information security culture and awareness	2016	Computers & Security
16	Safa, Von Solms & Furnell	Information security policy compliance model in organizations	2016	Computers & Security
17	Siponen, Mahmood & Pahnila	Employees' adherence to information security policies: An exploratory field study	2014	Information & Management
18	Tsohou et al.	Analyzing trajectories of information security awareness	2012	Information Technology & People
19	Tsohou et al.	Managing the introduction of information security awareness programmes in organizations	2015	European Journal of Information Systems
20	Vance, Siponen & Pahnila	Motivating IS security compliance: Insights from Habit and Protection Motivation Theory	2012	Information & Management

Appendix I. Articles selected for review