Organizational practices as antecedents of the information security management performance: An empirical investigation

Abstract

Purpose– The purpose of this paper is to expand current knowledge about the security organizational practices and analyse its effects on the Information security management performance

Design/methodology/approach– Based on the literature review, the authors propose a research model together with hypotheses. The survey questionnaires were developed to collect data, which then validated the measurement model. The authors collected 111 responses from CEOs at manufacturing SMEs that had already implemented security policies. The hypothesized relationships were tested using the structural equation model approach with EQS 6.1 software.

Findings– Results validate that Information security knowledge sharing, Information security education and Information security visibility, as well as security organizational practices, have a positive effect on the information security management performance.

Research implications– The consideration of organizational aspects of information security that should be taken into account by academics, practitioners and policymakers in SMEs. Besides, the work helps validate novel constructs used in recent research (Information Security knowledge sharing and Information security visibility).

Originality/value –The literature recognizes the need to develop empirical research on information security focused on SMEs. Besides to the need to identify organizational practices that improve information security. This paper empirically investigates SMEs organizational practices in security of information and analyse its effects on the performance of information security.

Security organizational practices, Information security knowledge sharing, Information security visibility, Information security education, performance of information security management, SMEs

1. Introduction

Digital interrelations fostered by the Internet, IoT, Cloud computing and other technologies, in which people and companies act as interconnected and interdependent nodes, have meant that information security has a strategic importance (Doherty and Fulford, 2005; Chen *et al.*, 2008; Cram *et al.*, 2017), especially in business environments, where the competitiveness of organizations depends on their ability to manage the information (Drucker, 2002; Gordon and Loeb, 2006; Preston and Karahanna, 2009; Soomro *et al.*, 2016).

Global spending on IT security in 2017 has increased to $96.3 billion at a growth rate of 8 percent, which doubles the rate of IT budgets over the last two years (Gartner, 2017). Organisations are increasingly focusing on implementing information security products such as anti-virus, intrusion detection and prevention systems, database/contents security, total security systems and public key infrastructure (Venter and Eloff, 2003; Cavusoglu *et al.*, 2009). Indeed, despite the prevalence of technical security measures, studies have reported that internal security incidents continue to happen and create more damage and losses than security incidents caused by outsiders (Baskerville *et al*., 2014).

In this sense, experts growingly argue that the main cause for information security incidents lies mainly with employees' behavioural and organizational factors rather than technical issues per se, which implies a turn to internal problems attributed to the organizational practices and users of information systems (Siponen *et al*., 2014; Soomro *et al*., 2016; Doherty and Tajuddin, 2018; Moody *et al*., 2018).

The literature on information security in companies has mainly focused on technological issues, and to a lesser extent on strategies, security standards and policies. Recent research indicates the need of a more holistic approach to understand information security management (Soomro *et al*., 2016; Cram *et al*., 2017; Doherty and Tajuddin, 2018).

In this sense, the literature points out the need for works that identify the organizational factors that affect the security of information. Thus, the works that describe a great variety of factors of organizational type are incipient and with a predominant qualitative analysis. These factors are business size, sector, information security policy, information security education, training, culture, behavior and compliance with security policy, awaraness, knowledge, visibility (Flores *et al*., 2014; Singh *et al*., 2014; Cram *et al*., 2017; Doherty and Tajuddin, 2018). The literature highlights the need to advance in the field of knowledge not only describing but also organizing the factors and analysing in an empirical way the effect they have on the performance of information security management. It is especially necessary to do it in small and medium-sized enterprises (SMEs) where there is a greater lack of work despite the fact that they are the most numerous business organizations in the developed economies, having an important contribution for the employment and productivity (OECD, 2009; Flores *et al*., 2014; Safa and Von Solms, 2016).

At present, the literature points out in different qualitative and revision studies a great variety of organizational factors, emphasizing especially their transversality, being common to all organizations regardless of size and sector, and having already been categorized through constructs in previous studies: Information security education, Information Knowledge sharing and Information security visibility (Singh *et al*., 2014; Soomro *et al*., 2016; *Choi* et al., 2018).

To address these issues, this paper aims to examine (empirically theorize and test) how companies can improve the performance of information security through organizational practices such as Information security education, Information Knowledge sharing and Information security visibility, in the specific context of industrial SMEs. The remainder of this article is organized as follows. The next section presents the referential background and hypotheses. Following that, the research methods, drawing from a large sample consisting of industrial SMEs, are described. Then, the data analysis and results are presented. Finally, the article ends with a discussion on the research findings, concluding remarks, limitations, and future research guidelines.

2. Theoretical background and hypotheses

The analysis of the information security is a complex subject due to its multidisciplinary character (Flores *et al*., 2014; Safa and Von Solms, 2016; Hwang *et al*., 2017). According to Soomro, Shah, and Ahmed (2016), a more holistic approach is needed for information security management. Siponen *et al*. (2014) suggest that information security issues should be considered in a management perspective.

In this sense, information security is a field which has been treated in literature especially by academics and information professionals. However, it is a relatively modern concept in the focus of business management (Dhillon and Backhouse, 2001; Gordon and Loeb, 2006) and has acquired a greater impact from the generalized use of Internet in business and the possibilities that the technologies based on Web allow in all enterprise process.

In this line, the analysis of the literature on information security in organizations shows that the treatment of this subject has evolved from technical to management approaches. Thus, the first references that studied the information security in companies were primarily focused on describing the information security from a technological approach and seeking technical tools to improve it (Kim *et al*., 2005; Kwon *et al*., 2007).

A major advance in the study of information security, with a focus on the company, has been produced in recent years with works without forgetting the technical aspects, considering organizational variables, analyzing issues related to compliance with the standards of information security, developing models and systems of information security management, and analyzing its certification (Siponen and Willison, 2009; May and Dhillon, 2010). These studies are important because they relate information security strategy to business processes and give rise to the consideration of information security as a process, whose development must start from the strategic level to the rest of the organization (Siponen and Willison, 2009; Werlinger *et al*., 2009; May and Dhillon, 2010; Singh *et al*., 2014).

Thus, it is especially important to identify the organizational aspects that are indicated in the information management security (Table 1). In this sense, the works that identify organizational factors that can affect the information security performance are recent. These works are varied in: methodology, mainly theoretical approaches and case studies; units of analysis, in general large organizations, and present a wide variety of factors deriving from the literature review itself, with the need to advance in this topic of study by organizing the factors and empirically analyzing their effects on the performance of information security management.

Table 1 Literature review Organizational factors in information security management

Whitman (2004)	Information security needs higher levels of awareness, education and policy
Chang and Ho (2006)	Quantify the impacts of organizational culture traits on the effectiveness of implementing ISM.
Hagen and Albrechtsen (2008)	Awareness-creating activities are applied by the organizations to a considerably lesser extent but at the same time these are assessed as being more effective organizational measures than technical-administrative ones.
Ma *et al*. (2009)	Information security training is possibly the most important measure for its effectiveness, as it increases awareness and understanding.
Puhakainen and Siponen (2010)	Information security policy compliance training has a positive effect on employees' Behaviour regarding compliance.
Albrechtsen and Hovden (2010)	Employee participation and knowledge creation incorporate positive changes towards information security awareness and behaviour.
Flores *et al*. (2014)	Authors present an empirical investigation on what behavioural information security governance factors drive the establishment of information security knowledge sharing in organizations.
Parsons *et al*. (2014)	Awareness training and education have positive impact on employee attitude and behaviour towards information security policy.
Singh *et al*. (2014)	The paper categorizes various organizational ISM functions into ten factors. Spanning across three levels (strategic, tactical and operational), these factors cover various management issues of organizational ISM.
Safa and Vol Solms (2016)	Information security knowledge sharing (ISKS) forms and decreases the risk of information security incidents.
Soomro *et al*. (2016)	Development and execution of information security policy, awareness, compliance training, development of effective enterprise information architecture, IT infrastructure management, business and IT alignment and human resources management, had a significant impact on the quality of management of information security.
Hwang *et al*. (2017)	The authors found that security systems, security education, and security visibility decrease instances of non-compliance.
Choi *et al*. (2018)	The paper identifies a set of organisational insiders' perceived components of effective information security practices (organisational mission statement; common understanding of information security; awareness of threats; knowledge of information security incidents, routines and policy; relationships between employees; circulation of stories; role of punishment provisions; and training), based on which more successful information security strategies can be developed.
Moody *et al*. (2018)	This paper reviews 11 theories that have served the majority of previous information security behavior models. It empirically compares these theories and proposes a unified model, called the unified model of information security policy compliance (UMISPC), which integrates elements across these extant theories.

According to Soomro *et al*. (2016), the quantity of articles in the last years shows that the research trend in exploring the management role in information security is growing. This approach is under construction and, within this approach the organizational role in information security is becoming increasingly important and is gaining the attention of researchers. This research is an attempt to contribute to filling the gap in the literature by focusing on the organizational practices. Specifically, the review of the literature stands out as the most cited, cross-cutting for any organization and constitutes practices at the operational level and the execution by all employees, the following: Information security knowledge sharing, Information security education, Information security visibility

Information security knowledge sharing

In relation to the above, recent studies place the focus of research on the role of shared knowledge in information security. Experts face similar problems in this domain and they should provide proper solutions for them. Preventing the development of the same solutions for similar problems by means of sharing knowledge. This practice leads to the avoidance of time-wasting and extra costs (Feledi *et al*., 2013). Sharing previous relevant experiences in the domain of information security is a valuable resource in information security awareness. (Rhee, *et al*., 2009; Safa and Von Solms, 2016).

In this context, information security knowledge sharing not only increases the level of awareness as an effective approach, but also reduces the cost of information security in organizations. Information security knowledge sharing refers to collaboration with others by sharing our experiences, ideas and knowledge in order to safeguard information assets in organizations (Flores *et al*., 2014). It includes periodic meetings of knowledge sharing, mail list, wikis and specific web spaces to share knowledge.

Therefore, this discussion leads to the following hypotheses:

Hypothesis 1: The organizational practice of Information security knowledge sharing is positively related to the performance of Information security management.

Information security education

Within the traditional organizational practices to improve the security of business information, is security education within the context of the organization itself, as reflected in the main information security standards (ISO/IEC 27001:2005; ITIL; COBIT; NIST Special Publication 800). Such standards coincide in pointing out the fundamental role that information security education has as an organizational factor that must ensure in the personnel a sufficient knowledge in security and contributes to reduce incidents, and thus has been treated in the literature (Siponen, 2000; Lee *et al*., 2004; DÀrcy *et al*., 2009). Information security education refers to a program or efforts to make employees aware of the environment, policy, and manual of an organization's security (Hwang *et al*., 2017). It includes in an organized and coordinated way talks, tailored educational materials, specific training and knowledge evaluation. Based on this discussion, the following hypothesis is proposed:

Hypothesis 2: Information security education efforts are positively related to the performance of Information security management.

Education in security information in the enterprise environment is important. Nevertheless, successful organizational education requires more actions aimed at complementing shared knowledge and education, for example through the visibility of the subject.

Information security visibility

Hwang *et al*. (2017) defined security visibility as the degree of organizational efforts to provide employees with a positive view of information security policies. The literature suggests that when organizations encourage the visibility of information security technologies, procedures, activities, and control methods, employees are able to voluntarily form a security culture (AlHogail, 2015; Faily and Fléchais, 2010; Lacey, 2010).

Information security policies, activities, incidents, and practices should be visible and continuously advertised to employees in order for them to make decisions that are consistent with the organization's desirable direction. Such visibility has an impact on the compliance of employees who are required to adhere to information security policies (Siponen *et al*., 2010; Hwang *et al*., 2017). Among others, posters, notices, press releases and bulletin boards are also included. Thus, the following hypothesis is suggested:

Hypothesis 3: Information security visibility in organizations is positively related to the performance of Information security management.

3. Research methodology

Data and sample

The organizations selected for this study are industrial SMEs from Cantabria, in the north of Spain, where economic, technological development and IT use is similar to other OECD regions and to the Europa average (OECD, 2017; European Commission, 2018). In this sense, this region has been selected because its social, economic and innovation variables are located within the average of Europe and the OECD. This situation facilitates the comparison with other regions (Fritsch and Wyrwich, 2018, Rodríguez-Pose and Wilkie, 2019).

With respect to SMEs, this kind of firms have been selected due to the relevance they have in the economy, representing more than 95% of companies of development economies (OECD, 2016). In contrast, there are insufficient works that analyze the organizational practices in information security and their effects on the security of information of this type of companies (Dutot *et al*., 2014). At the same time, international organizations' reports suggested that the industrial sector is behind the implementation of new IT development in its information security processes, and therefore, there is some space for improvement (OECD, 2016). Besides, in developed countries, there is an urgent need for improving the competitiveness of this sector (OECD, 2016).

To ensure a minimum firm complexity in which IT may be relevant, the population considered in this study was industrial SMEs, with 10 employees or more, located in the region of Cantabria. A total of 478 SMEs were identified, for this purpose, the official database of the Cantabria Institute of Statistics (ICANE, 2016) was used. All the SMEs identified were invited by email to participate in the study. A personal interview was conducted to the companies that showed interest. In total, 111 valid questionnaires were obtained, yielding a response rate of 23.2%. The sample characteristics are presented in Table 2.

Data collection was conducted following two phases. First, a pilot study was performed, and, following that, a questionnaire was conducted. Five SMEs were randomly selected from a database to perform the pilot study. Based on these responses and the subsequent interviews with the participants in the pilot study, minor modifications were made to the questionnaire for the next phase of data collection. Responses from these five pilot-study firms were not included in the final sample. The survey was administered to the CEO of the companies via personal interview and the company was the unit of analysis for this study. All answers were treated anonymously and confidentially. The technical research summary is presented in Table 3.

Table 2. Sample characteristics.

Intervals	% in total	% in total	Average value
Employees			
10–49	80.1	89	46
50–249	19.9	22	
Total	100	111	
Sales (€)			
0 ≤ 500000	28	31	€ 1,1 million
500001 ≤ 1 million	47.7	53	
>1 million	24.3	27	
Total	100	111	
Age (years)			
0 ≤ 9	7.2	8	23
10 ≤ 20	55	61	
>20	37.8	42	
Total	100%	111	

Table 3. Research technical summary

Pilot study	Random sampling five SMEs from a database, February 2016
Quantitative study (survey)	
Universe	478 SMEs from the industrial with 10 employees or more
Sampling procedure	All the companies that formed the universe were contacted
Collection of information	Survey administrated to the CEO via personal interview
Unit of analysis	Was the company
Date of field work	111 valid questionnaires (response rate of 23.2%)
Sampling error	8.16%
Level of trust	95.5% (K = 1.96) for the most unfavorable case p = q = 0.5
Date of field work	February –July 2016

Measures

Measurement items were introduced on the basis of a careful literature review. Constructs and associated indicators in the measurement model are listed in the Appendix and discussed below. To facilitate future research, scales of measure tested by previous studies were used. Scales were measured on a 5-point Likert scale with anchors from strongly disagree (1) to strongly agree (5). All the variables were operationalized as multi-item constructs.

The *Information Security Knowledge Sharing* measured the level at which an organization has established processes to capture and share knowledge about information security among organizational members through formal and informal information flows (Belsis *et al*., 2005; Zakaria, 2006, Flores *et al*., 2014). Items for this variable are based on Flores et al. (2014).

Information Security Education assessed the extent to which companies used education activities or efforts to make employees aware of the environment, policy, and manual of an organization's security (Lee *et al*., 2004; Hwang *et al*., 2017). This variable was operationalized based on Hwang *et al*. (2017).

Information Security Visibility measured the degree of organizational efforts to provide employees with a positive view of information security policies (AlHogail, 2015; Faily and Fléchais, 2010; Lacey, 2010). Security visibility scale is based on Siponen *et al*. (2010) and Hwang *et al*. (2017).

The information Security Performance measured the degree in which the information security program achieves its goals and the information is sufficiently protected. This includes preventing multiple cybercrime options, among other viruses, malware, hackers, Trojan, phishing or ransomware. The variable was operationalized following the items used in previous studies, such as: Straub, (1990); Knapp *et al*. (2007); Khan *et al*. (2011); Zhang *et al*. (2012) and Trigueros-Preciado *et al*. (2013).

Instrument validation

The measures from the dataset were refined by assessing their unidimensionality and reliability. First, an initial testing of unidimensionality was made using principal component factor analyses. In each analysis, eigenvalues were greater than 1, lending preliminary support to a claim of unidimensionality in the constructs. Next, a confirmatory factor analysis (CFA) was performed to assess the required convergent validity, discriminant validity, and reliability of the constructs. This study uses EQS 6.1 to estimate the measurement model. The measurement model presented a good fit to the data (χ2(21)= 32.479, p=0.152; CFI = 0.96; IFI = 0.96; GFI = 0.95; RMSEA = 0.06). All traditionally reported fit indexes were within the acceptable range. This study calculated reliability of measures, using Bagozzi and Yi's (1998) composite reliability index, and Fornell and Larcker's (1981) average variance extracted index.

For all the measures, both indexes were higher than the evaluation criteria, namely 0.7 for composite reliability and 0.5 for the average variance extracted. With regard to convergent, all estimated standard loadings are significant (p<0.01) and of acceptable magnitude (see Table 4), suggesting good convergent validity. Furthermore, the Cronbach´s Alpha values of all indicators exceed the recommended value of 0.6 (Hair *et al*., 1999).

Table 4. Measurement model: Confirmatory analysis, scale reliability and convergent validity

Construct	Indicator	S. Loadings	t-value	Cronbach´s Alpha	Reliability
Information Security Knowledge Sharing	ISKS1	0.92	-	0.87	CR=0.89 AVE=0.72
	ISKS2	0.88	16.32		
	ISKS3	0.74	9.18		
Security education	SE1	0.84	-	0.84	CR=0.85 AVE=0.65
	SE2	0.68	8.42		
	SE3	0.88	10.73		
Security visibility	SV1	0.65	-	0.81	CR=0.81 AVE=0.60
	SV2	0.89	6.49		
	SV3	0.82	6.46		
Information security effectiveness	ISE1	0.86	-	0.90	CR=0.90 AVE=0.58
	ISE2	0.77	14.08		
	ISE3	0.73	9.64		
	ISE4	0.64	6.77		

Note. Fit statistics for measurement model: χ2(21)= 32.479, p=0.152; CFI = 0.96; IFI = 0.96; GFI = 0.95; RMSEA = 0.06; (-) Fixed Items; CR: Composite reliability. AVE: Average variance extracted

To assess the discriminant validity, the Fornell and Larcker's (1981) criterion was used. This criterion involves that the square root of average variance extracted for each construct (diagonal elements of the correlation matrix in Table 5) should be greater than the absolute value of inter-construct correlations (off-diagonal elements). All constructs met this criterion, suggesting that the items share more variance with their respective constructs than with other constructs. Table 5 also provides an overview of the average, standard deviations and correlations of the constructs.

Table 5. Descriptive statistics and discriminant validity

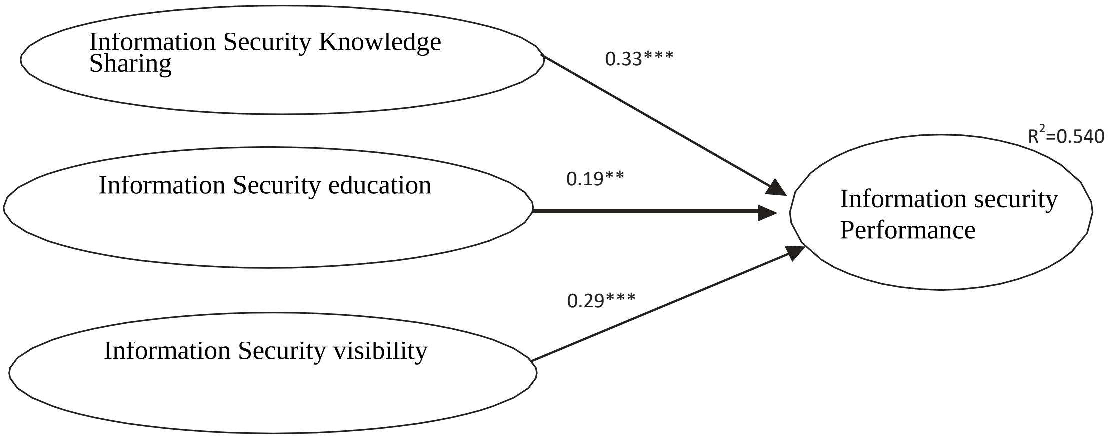
Construct	Av.	SD	Correlation matrix			
			(1)	(2)	(3)	(4)
1. Information Security Knowledge Sharing	2.85	1.11	**0.81**			
2. Security education	3.052	1.39	0.58	**0.84**		
3. Security visibility	2.61	1.62	0.47	0.70	**0.77**	
4. Information security effectiveness	2.42	1.47	0.33	0.56	0.71	**0.72**

Note. Av. Average score of all items includes in the construct. SD standard deviation; Diagonal values in bold represent the square root of the AVE

4. Results

This article estimated the structural model (SEM) with the EQS 6.1 software package using maximum likelihood estimation techniques to test the model (SEM-ML). The fit of the model is satisfactory (χ2(17) = 29.982, p = 0.183; RMSEA = 0.053; CFI = 0.99; IFI = 0.99; GFI = 0.98), suggesting that the nomological network of relations fits the data and the validity of the measurement scales. Figure 1 shows the standardized path coefficients with their respective significant levels.

Figure 1. Empirical results


Information Security Knowledge Sharing
0.33***
R^2=0.540
Information Security education
0.19**
Information security Performance
0.29***
Information Security visibility

Notes:***<p0.01; **p<0.05

Table 6. Summary of hypotheses test

Hypothesis		Path coefficient	*P* value	Result
H1	Organizational practice of Information security knowledge sharing is positively related to the performance of Information security management.	0.33	<0.01	Support
H2	Information security education efforts is positively related to the performance of Information security management.	0.19	<0.05	Support
H3	Information security visibility in organizations is positively related to the performance of Information security management.	0.29	<0.01	Support

Hypothesis 1 was supported (0.33, p < 0.01), indicating that Information Security Knowledge Sharing is related to the Information security performance in SMEs. This is the strongest factor in the proposed model. This indicates that the Information Security Knowledge Sharing is a critical factor to the performance of information security in industrial SMEs.

Hypothesis 2 was supported (0.19, p < 0.05), indicating that Security education is related to the performance of information security in SMEs, although it is the weakest relation of the model.

Hypothesis 3 was supported (0.29, p < 0.01). This result shows that Security visibility in the firm is an important factor for the performance of information security in SMEs.

Implications of these results are discussed in the next section.

5 Discussion

This paper investigates the effects of information security organizational practices (Information security knowledge sharing, Information security education, Information security visibility) on the performance of Information security management in industrial SMEs.

The first finding shows the security education is weakly related to the extent of performance of information security. A possible explanation to this can be the set of companies, SMEs, and the sector of the sample, industrial. In Spain, the majority of this type of company subcontracts training in information security, which can be seen by employees as a non-important and complementary task. In any case, the results are consistent with previous research such as Siponen *et al*. (2010) and Hwang *et al*. (2017).

Regarding the Information security knowledge sharing, results suggested that it is positively associated with the performance of information security of SMEs. This finding supports recent research such as Flores *et al*., (2014) and Tatu *et al*., (2018) which found that Information Security Knowledge Sharing are adequate tools to improve information security in organizations.

With regard to the Information Security visibility, its effect on the performance of information security management of SMEs is analyzed. The results show a positive relation between these two constructs. This finding confirms novel previous research (Hwang *et al*., 2017). Thus, performance of information security in industrial SMEs emerges from Information Security Knowledge Sharing and information security visibility, rather than from education.

6. Conclusions, limitations and future research

The competitiveness of SMEs depends on their ability to secure management of their main asset, information, and, because of this, they need to have adequate security organizational practices beyond just technological resources.

Thus, this study extends the analysis of information security in SMEs beyond traditional theories and examines concrete organizational practices such as Information security knowledge sharing, Information education and Information security visibility, by analysing the effects of these three organizational practices on the performance of information security in industrial SMEs.

This paper provides with several implications to the academics:

First, this paper extends the theoretical development and empirical evidence on information security initiatives at firm level by focusing on knowledge sharing, education, and visibility. Prior Information security research has focused more on the technological dimension of IT security practices. This paper focuses on the organizational dimension of information security practices.

Second, this paper focuses on SMEs. Previous studies in the literature tend to focus in large businesses, with very few and recent studies analysing concrete organizational security practices use in SMEs. In addition, this work goes beyond the usual case studies as it is based on a large sample of SMEs.

Third, we extend previous works by analysing how security organizational practices affect the performance of information security. Our results suggest that an improved performance of information security in the industrial SMEs requires innovative practices to foster knowledge sharing among employees. Besides, in line with previous works, the positive relation between the information security visibility and the performance of information security management is showed. This finding contributes to the security management field by offering an explanation of the performance of information security within a particular sector. Moreover, the findings significantly contribute to the literature by considering organizational aspects of information security that should be taken into account by both academic and practitioners.

Fourth, in the line of previous works (e.g., Benitez *et al.* 2018), this paper contributes to IS literature on IT business value by theorizing and demonstrating how investment in organizational information security practices improves its performance which, in turn, helps companies to create business value from IT.

With respect to the practical implications for the industry:

This work relates information security to organizational variables that are comprehensible for managers and can serve as an example to show how information security can be more than technology and how the security of information is associated with organizational practices that positively affect the information security and value generation. The work specifically shows that an appropriate improvement of the personnel knowledge sharing is needed to improve the information security in the industrial SMEs. Making them aware of the importance of information security and its relationship with the business processes is also needed, since these factors brake the development of information security in the companies.

With respect to the practical implications for the policymakers:

Government programs and grants to help companies improve information security focus on supporting companies in the purchase of hardware and software technology solutions, without paying attention to organizational issues. However, this work highlights the importance of the organizational factors regarding information security performance, which should be taken into account when designing plans and information security aids. In particular, the work shows that directing aids and designing plans that improve shared knowledge on information security and the issues that give visibility to the subject of information security will allow companies to improve their information security performance.

To conclude, while the contributions of the present study are significant, we would acknowledge that this study has some limitations, which could be addressed in future research. First, the sample used was from Spain. This means that the findings could be extrapolated to other countries, since economic and technological development in Spain is similar to other OECD Member countries. However, in future research, a sampling frame that combines firms from different countries could be used in order to provide a more international perspective on the subject. Second, the sample consisted of small and medium sized enterprises (SMEs). As SMEs are characterized by having less technological resources than their higher-level counterparts (large firms), this may influence the extent of sophistication in the security practices use. Therefore, in future works, the segment of large companies is worth special analysis. Third, the key informant method was used for data collection. This method, while having its advantages, also suffers from the limitation that the data reflects the opinions of one person. Future studies could consider research designs that allow data collection from multiple respondents within an organization. Fourth, it takes a static, cross-sectional picture. A longitudinal study could enrich the findings. Related to the foregoing, as future research lines, it would be interesting to replicate this work in other sectors, like service companies. These suggestions should be taken into account in future studies to increase the validity of our findings.

Appendix A. Measures

Information Security Knowledge Sharing	ISKS1	In our company, employees frequently share their experiences about information security
	ISKS2	In our company, employees frequently share their expertise from their information security training with their colleagues
	ISKS3	In our company, employees frequently talk with others about information security incidents and their solutions in our meetings
Security education	SE1	Our organization provides employees with appropriate security education before giving them authorized access to the corporate network
	SE2	Our organization provides employees with proper security education on risks associated with internet usage
	SE3	Our organization provides employees with education on the proper usage of technologies associated with information
Security visibility	SV1	In our organization, information security activities are advertised widely
	SV2	In our organization, information security incidents are visible in public
	SV3	In our organization, good information security practices are advertised in public
Information security effectiveness	ISE1	The information security program achieves most of its goals
	ISE2	Overall, the information security program is effective
	ISE3	The information security program has kept risks to a minimum
	ISE4	The number of information security problems has decreased in the last year

Note. (1-5): five-point Likert-type scales

References

Ahmad, A., Bosua, R. and Scheepers, R. (2014), "Protecting organizational competitive advantage: a knowledge leakage perspective", *Computers & Security*, Vol. 42, pp. 27-39.

Albrechtsen, E. and Hovden, J. (2010), "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers & Security*, Vol. 29 No.4, pp. 432-445, available at: https://doi.org/10.1016/j.cose.2009.12.005

AlHogail, A. (2015), "Design and validation of information security culture framework", *Computers in Human Behavior*, Vol. 49, pp. 567-575, available at: https://doi.org/10.1016/j.chb.2015.03.054

Bagozzi, R.P. and Yi, Y. (1998), "On the evaluation of structure equation models", *Journal of the Academy of Marketing Science*, Vol. 16 No. 1, pp. 74-94, available at: https://doi.org/10.1007/BF02723327

Baskerville, R., Spagnoletti, P. and Kim, J. (2014), "Incident-centered information security: Managing a strategic balance between prevention and response", *Information & Management*, Vol. 51 No. 1, pp. 138-151.

Belsis, P., Kokolakis, S. and Kiountouzis, E. (2005) "Information systems security from a knowledge management perspective", *Information Management & Computer Security,* Vol. 13 No. 3, pp.189-202, available at: https://doi.org/10.1108/09685220510602013

Benitez, J., Ray G. and Henseler J. (2018), "Impact of information technology infrastructure flexibility on mergers and acquisitions", *MIS Quarterly*, Vol. 42 No. 1, pp. 25-43.

Burns, A.J., Posey, C., Courtney, J.F., Roberts, T.L. and Nanayakkara, P. (2017), "Organizational information security as a complex adaptive system: Insights from three agent-based models", *Information Systems Frontiers*, Vol. 19 No. 3, pp. 509-524.

Cantabria Institute of Statistics, ICANE (2016), available at: https://www.icane.es (accessed 26 April 2019).

Cavusoglu, H., Raghunathan, S. and Cavusoglu, H. (2009), "Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems", *Information System Research,* Vol. 20 No. 2, pp. 198-217.

Chang, S.E. and Ho, C.B. (2006), "Organizational factors to the effectiveness of implementing information security management", *Industrial Management & Data Systems*, Vol. 106 No. 3, pp. 345-361, available at: https://doi.org/10.1108/02635570610653498

Chen, R., Sun, C., Helms, M.M. and Jih, W. (2008), "Aligning information technology and business strategy with a dynamic capabilities perspective: a longitudinal study of a taiwanese semiconductor company", *International Journal of Information Management*, Vol. 28 No. 5, pp. 366-378.

Choi, S., Martins, J.T. and Bernik, I. (2018), "Information security: Listening to the perspective of organisational insiders", *Journal of Information Science*, Vol. 44 No. 6, pp. 752-767, available at: https://doi.org/10.1177/0165551517748288.

Cram, W.A., Proudfoot, J.G. and D’Arcy, J. (2017), "Organizational information security policies: a review and research framework", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 605-641.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127-153.

Doherty, N.F. and Fulford, H. (2005), "Aligning the information security policy with the strategic information systems plan", *Computers & Security,* Vol. 25 No.1, pp. 55-63.

Doherty, N.F. and Tajuddin, S.T. (2018), "Towards a user-centric theory of value-driven information security compliance", *Information Technology & People*, Vol. 31 No. 2, pp. 348-367.

Drucker, P.F. (2002), *Managing in the Next Society*, St. Martin´s Press, New York, NY.

Dutot, V., Bergeron, F. and Raymond, L. (2014), "Information management for the internationalization of SMEs: An exploratory study based on a strategic alignment perspective", *International Journal of Information Management,* Vol. 34 No. 5, pp. 672-681.

European Commission (2018), Science, Research and Innovation Performance of the EU 2018 Strengthening the Foundations for Europe's Future, European Commission, Luxembourg, available at: https://bit.ly/2EV6QU3 (accessed 9 May 2019).

Faily, S. and Fléchais, I. (2010), "Designing and aligning e-Science security culture with design", *Information Management & Computer Security*, Vol. 18 No. 5, pp. 339-349, available at: https://doi.org/10.1108/09685221011095254

Feledi, D., Fenz, S. and Lechner, L. (2013), "Toward web-based information security knowledge sharing", Information Security Technical Report, Vol. 17 No. 4, pp. 199-209.

Flores, W.R., Antonsen, E. and Ekstedt, M. (2014), "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture", *Computers & Security*, Vol. 43, pp. 90-110, available at: https://doi.org/10.1016/j.cose.2014.03.004

Fornell, C. and Larcker, D.F. (1981), "Structural equation models with unobservable variables and measurement error: Algebra and statistics", *Journal of Marketing Research*, Vol. 18 No. 3, pp. 382-388, available at: https://doi.org/10.1177/002224378101800313

Fritsch, M. and Wyrwich, M. (2018), "Regional knowledge, entrepreneurial culture, and innovative start-ups over time and space—an empirical investigation", *Small Business Economics*, Vol. 51 No. 2, pp. 337-353, available at: https://doi.org/10.1007/s11187-018-0016-6

Gartner (2017), *Forecast: Information Security, Worldwide, 2015-2021, 3Q17 Update*, Gartner Research, available at: https://www.gartner.com/en/documents/3825766 (accessed 5 May 2019).

Gordon, L.A. and Loeb, M.P. (2006), "Economic aspects of information security: An emerging field of research", *Information Systems Frontiers*, Vol. 8 No. 5, pp.335-337.

Hagen, J.M. and Albrechtsen, E. (2008), "Implementation and effectiveness of organizational information security measures", *Information Management & Computer Security*, Vol. 16 No. 4, pp. 377-397, available at: https://doi.org/10.1108/09685220810908796

Hair, J.F., Anderson, R.E., Tatham, R.L. and Black, W.C. (1999), *Análisis Multivariante*, Prentice Hall, Madrid.

Hwang, I., Kim, D., Kim, T. and Kim, S. (2017), "Why not comply with information security? An empirical approach for the causes of non-compliance", *Online Information Review*, Vol. 41 No.1, pp. 2-18, available at: https://doi.org/10.1108/OIR-11-2015-0358

ISO/IEC 27001:2005, *Information technology - Security techniques - Information security management systems - Requirements*, International Standard Organization.

ISO/IEC 27032:2012, *Information technology - Security techniques - Guidelines for cybersecurity*, International Standard Organization.

Kim, S., Leem, C.S. and Lee, H.J. (2005), "An evaluation methodology of enterprise security management systems", *International Journal of Operations and Quantitative Management*, Vol. 11 No. 4, pp. 303-312.

Khan, M.K., Kim, S-K. and Alghathbar, K. (2011), "Cryptanalysis and security enhancement of a ‘more efficient & secure dynamic ID-based remote user authentication scheme’", *Computer Communications*, Vol. 34 No. 3, pp. 305-309, available at: https://doi.org/10.1016/j.comcom.2010.02.011

Knapp, K.J., Marshall, T.E., Rainer Jr., R.K. and Ford, F.N. (2007), "Information security effectiveness: Conceptualization and validation of a theory", *International Journal of Information Security and Privacy*, Vol. 1 No.2, pp. 37-60, available at: https://doi.org/10.4018/jisp.2007040103

Kwon, S., Jang, S., Lee, J. and Kim, S. (2007), "Common defects in information security management system of Korean companies", *Journal of Systems and Software*, Vol. 80 No. 10, pp. 1631-1638, available at: https://doi.org/10.1016/j.jss.2007.01.015

Lacey, D. (2010), "Understanding and transforming organizational security culture", *Information Management & Computer Security*, Vol. 18 No. 1, pp. 4-13, available at: https://doi.org/10.1108/09685221011035223

Lee S.M., Lee S-G. and Yoo S. (2004), "An integrative model of computer abuse based on social control and general deterrence theories", *Information & Management,* Vol. 41 No. 6, pp. 707-718, available at: http://dx.doi.org/10.1016/j.im.2003.08.008

Ma, Q., Schmidt, M.B. and Pearson, J.M. (2009), "An integrated framework for information security management", *Review of Business,* Vol. 30 No. 1, pp. 58-69.

May, J. and Dhillon, G. (2010), "A holistic approach for enriching information security analysis and security policy formation", in *Proceedings of the 18th European Conference on Information Systems* (*ECIS 2010) in Pretoria, South Africa, 7-9 June 2010,* Paper 146. available at: http://aisel.aisnet.org/ecis2010/146 (accessed 10 May 2019).

Moody, G.D., Siponen, M. and Pahnila, S. (2018), "Toward a unified model of information security policy compliance", *MIS Quarterly,* Vol. 42 No. 1, pp. 285-311, available at: https://doi.org/10.25300/MISQ/2018/13853

OECD (2009), *The Impact of the Global Crisis on SME and Entrepreneurship Financing and Policy Responses*, OECD Centre for Entrepreneurship, SMEs and Local Development, Paris, available at: http://www.oecd.org/dataoecd/40/34/43183090.pdf (accessed 6 May 2019).

OECD (2016), *Financing SMEs and Entrepreneurs 2016: An OECD Scoreboard*, OECD Publishing, Paris.

OECD (2017), *OECD Economic Surveys: Spain*, OECD Publishing, Paris.

Park, S. and Ruighaver, T. (2008), "Strategic approach to information security in organizations", in *Proceedings of the 2008 International Conference on Information Science and Security (ICISS 2008) in Seoul, Korea, 10-12 January*, IEEE Computer Society, Washington DC.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q) ", *Computers & Security*, Vol. 42, pp. 165-176, available at: https://doi.org/10.1016/j.cose.2013.12.003

Preston, D.S. and Karahanna, E. (2009), "Antecedents of IS strategic alignment: a nomological network", *Information Systems Research*, Vol. 20 No. 2, pp. 159-179.

Puhakainen, P. and Siponen, M. (2010), "Improving employees' compliance through information systems security training: An action research study", *MIS Quarterly*, Vol. 34 No. 4, pp. 757-778, available at: https://doi.org/10.2307/25750704

Rhee, H-S., Kim, C. and Ryu, Y.U. (2009), "Self-efficacy in information security: Its influence on end users' information security practice behaviour", *Computers & Security*, Vol. 28 No. 8, pp. 816-826. available at: https://doi.org/10.1016/j.cose.2009.05.008

Rodríguez-Pose, A. and Wilkie, C. (2019), "Innovating in less developed regions: What drives patenting in the lagging regions of Europe and North America", *Growth and Change*, Vol. 50, pp. 4-37, available at: https://doi.org/10.1111/grow.12280

Safa, N.S. and Von Solms, R. (2016), "An information security knowledge sharing model in organizations", *Computers in Human Behavior*, Vol. 57, pp. 442-451, available at: https://doi.org/10.1016/j.chb.2015.12.037

Singh, A.N., Gupta, M.P. and Ojha, A. (2014), "Identifying factors of “organizational information security management”", *Journal of Enterprise Information Management*, Vol. 27 No. 5, pp. 644-667, available at: https://doi.org/10.1108/JEIM-07-2013-0052

Siponen, M. (2000), "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*, Vol. 8 No. 1, pp. 31-41.

Siponen, M. and Willison, R. (2009), "Information security management standards: problems and solutions", *Information & Management*, Vol. 46 No. 5, pp. 267-270.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2014), "Employees’ adherence to information security policies: An exploratory field study", *Information & Management*, Vol. 51 No. 2, pp. 217-224.

Siponen, M., Pahnila, S. and Mahmood, M.A. (2010), "Compliance with information security policies: An empirical investigation", *Computer*, Vol. 43 No. 2, pp. 64-71, available at: https://doi.org/10.1109/MC.2010.35

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: A literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225.

Straub, D.W. (1990), "Effective IS security: An empirical study", *Information Systems Research*, Vol. 1 No. 3, pp. 255-276, available at: https://doi.org/10.1287/isre.1.3.255

Tatu, T., Ament, C. and Jaeger, L. (2018), "Lessons learned from an information security incident: A practical recommendation to involve employees in information security", Proceedings of the 51st Hawaii International Conference on System Sciences, pp. 3736-3745, available at: https://doi.org/10.24251/HICSS.2018.471

Trigueros-Preciado, S., Pérez-González, D. and Solana-González, P. (2013), "Cloud computing in industrial SMEs: Identification of the barriers to its adoption and effects of its application", *Electronic Markets*, Vol. 23 No. 2, pp. 105-114.

Venter, H.S. and Eloff, J.H. (2003), "A taxonomy for information security technologies", *Computers & Security*, Vol. 22 No. 4, pp. 299-307.

Werlinger, R., Hawkey, K. and Beznosov, K. (2009). "An integrated view of human, organizational, and technological challenges of IT security management", *Information Management & Computer Security*, Vol. 17 No.1, pp. 4-19.

Whitman, M.E. (2004), "In defense of the realm: understanding the threats to information security", *International Journal of Information Management*, Vol. 24 No. 1, pp. 43-57, available at: https://doi.org/10.1016/j.ijinfomgt.2003.12.003

Zakaria O. (2006), Internalisation of information security culture amongst employees through basic security knowledge. In: Fischer-Hübner, S., Rannenberg, K., Yngström, L., Lindskog, S., editors. Secur Priv Dyn Environ, Kluwer Academic Publishers, Boston.

Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J. and Deng, H. (2012), "A survey of cyber crimes", *Security and Communication Networks*, Vol. 5 No. 4, pp. 422-437.