Strategy of information security in small and medium enterprises, an technology-enterprise approach: analysis of its relationship with organizational and performance business variables

Daniel Pérez González*, Pedro Solana González** and Sara Trigueros Preciado***

*Department of Business Administration, University of Cantabria,
Avda. Los Castros s/n. 39005 Santander, Spain
E-mail: daniel.perez@unican.es

**Department of Business Administration, University of Cantabria,
Avda. Los Castros s/n. 39005 Santander, Spain
E-mail: pedro.solana@unican.es

***Department of Business Administration, University of Cantabria,
Avda. Los Castros s/n. 39005 Santander, Spain
E-mail: Sara.Trigueros@bshg.com

Abstract

The literature indicates a lack of strategic consideration for the information security in the organizations and two major gaps in the study of this subject: 1º the need to analyze the information security with multidisciplinary approaches, linking this issue with the business variables that managers understand; 2º extending the studies to SMEs, because despite its importance in the economy are falling behind on the information security. This paper analyzes the information security policy as a process that links business and technological strategies of the organizations. From this point, research is conducted in 78 industrial SMEs by analyzing: first, the degree of knowledge and application of information security policy and the issues that affect their strategic consideration and second, the contribution of the security policies of information to the value generation, finding positive evidence in this regard.

Key Words: Information security, strategy and policies of security, SME, business variables.

1. Introduction

The development of the information society and knowledge involves a continuous digitalization of all fields of human activity, especially in business and economic environments, where the competitiveness of organizations depends, to a large degree, on their ability to manage the information [1, 2, 3, 4].

This context of digital interrelations fostered by the Internet, in which people, governments and companies act as interconnected and interdependent nodes, has meant that the information security is acquiring a strategic importance [5, 6, 7], as a dynamic process that facilitates the protection of the main assets of organizations, so those that are unable to manage the information will be affected in all their critical processes – customers, suppliers, internal processes – and stop operating [8, 9, 10].

In this sense, information security has been talked about for some time, but mainly in technological terms aimed at looking for technical solutions and tools to apply [11, 7, 12]. In

recent years, the direction of research related to information security has evolved towards questions that, without forgetting the technical aspects, have begun to consider organizational variables, firstly by analyzing matters relating to compliance with information security standards, the development of models and management systems for information security and their certification [13, 14, 15, 16], and then studying real cases where information security has been applied in large companies and public bodies [17, 18]. Nevertheless, the majority of the work continues to be centred on analyzing information security from a technical viewpoint, especially in matters relating to security on the Internet [19, 20, 21] and studies that take business approaches are centred mainly on analyzing the costs and benefits that they have for companies investing in security [22] and the impact on the image or the valuation of a company's shares when the existence of security problems is leaked to the public [23, 24]. So, literature contains two approaches – technological and business –– in researching information security which necessarily should complement each other.

In this sense, information security is recognized as a process [25, 26, 27, 14] which is developed within an organizational context from which it cannot be isolated and which it affects completely, a process in which both people and technologies are prominently involved. Therefore, given that information security is a matter that affects the entire organization, it is necessary to do a deeper study and enhance the analysis with interdisciplinary approaches that allow the combination of technological, organizational and business variables that improve their understanding and application by companies [28, 3, 29]. In fact, various reports indicate that the absence in managers of a sufficiently broad and complementary vision – technological and business – is an important factor that makes it difficult for information security to play the role which, due to its importance, it should do [30, 31, 32].

Together with the previous need, the analysis of literature also reveals an important gap or deficit in academic and professional works centred on analyzing questions relating to information security and its application in SMEs [8, 33, 34], a deficit that it is necessary to deal with inasmuch as it is the SMEs that are the most numerous business organizations in developed economies [30]. Specifically in Spain, they represent 99.88% of all companies [35], very similar to what is happening in the European Union where according to the European Commission more than 99% of all businesses are SMEs providing two out of three of private sector jobs and contribute to more than half of the total value-added created by businesses in the EU. For that reason, agencies such as the [36, 9, 30] insist on the need to develop policies, studies and research that analyze information security in these organizations. In addition, the study of information security in SMEs is of interest because of the special characteristics of this type of company, normally with less available resources than the large

companies, which hinders their investment in management of information security and the alignment between information security and company strategy through a policy of security [37, 38].

Given the situation described, the objective of this work is to analyze, using a sample of 78 industrial SMEs, the degree of knowledge that they have on information security policies and delve deeper into organizational matters that indicate which factors are slowing up their implementation and which characterize the companies that apply these policies. Also, it studies whether having a security policy contributes effectively to the improvement of information security and the generation of value in organizations, using organizational and business performance variables to do this.

To achieve the above objectives, the work is structured in the following sections. Firstly, a review of the literature that analyses the concept of information security strategy and policy from which the research starts is carried out. Secondly, the methodology followed in the research is presented along with the results obtained, divided into two parts. The first part is more descriptive about the knowledge and application of security policies that companies have and what slows them down. The second part is made up of statistical inference with ANOVA models, to analyze whether the security policy contributes to the generation of value, which allows us to finish with the conclusions reached by the work, the limitations and future lines of investigation.

2. Review of Literature and Evolution of Information Security

Information security is a field which has been treated in literature especially by academics and information professionals, but it is a relatively modern concept in the environment of Management [39, 3] and has acquired a greater impact from the generalized use of the Internet in business and from the possibilities of interconnection that the Web allows.

Nevertheless, despite the recognition of its importance, the reports and statistics from international organizations show that there is still a lot of work to do in matters of information security, especially in small and medium companies (SMEs), where the rate of adopting security strategies and policies is lower than 21% [30, 40]. In this regard, there are various reports and authors that show that the relatively low development of information security in companies is motivated mainly by a lack of alignment between information security and business strategy and by the lack of management knowledge about the interrelation between information security and the business [28, 41, 30, 12, 32].

In this sense, the internationally recognized standards and management models for information security have a bearing on the need to consider information security in organizations as a process, whose development should start at the strategic level of the

organization [26, 14]. Therefore, in the first place it is of interest to specify the concept of security strategy and policy inasmuch as this acts as the driver of information security in organizations.

In this regard, the analysis of the information security strategy is a complex subject due to its multidisciplinary character [42] and little discussed in security literature by comparison with other subjects of a more technical nature [7].

In recent years, there have been works that show the need for information security to be aligned with the company strategy by means of an appropriate policy of information security [43, 6, 44, 7]. This way of understanding information security will make it possible for information security to attain the importance that it really has in companies and stop it being considered exclusively as a matter for the IT department and isolated from the rest of the organization [5, 41, 42].

In literature, many different definitions of security strategy can be found. [5] states that information security strategy should be formulated with a focus on management, linked to the corporate strategy more than to a technical approximation, which will allow the definition of long-term security policies and the development of efficient procedures. For [45], information security strategy means a long-term commitment that should come to fruition on the basis of resources, business requirements and the context of each company and which is, therefore, unique for each organization. One definition that stands out for its broad approach is that proposed by [7] for whom information security strategy is "*an art of deciding how to best utilize what appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defend organization's information infrastructure(s) against internal and external threats by offering confidentiality, integrity and availability at the expense of least efforts and costs while to be effective*".

Table 1 summarizes the main work and analysis carried out in recent literature on information security strategy and policies in a business context.

Table 1. Information security strategy and policies in recent literature

Authors	Objective of the analysis	Problem	Conclusions
[46]	Analysis of security policy on the basis of international standards.	Differences in the different standards with regards to the meaning and specific content of the security policy document.	Security policy as a fundamental document of information security. Standards and companies should work together in defining what the security policy should be.
[5]	Study of relationships between corporate culture, security strategy and the BS7799 standard.	Senior management in companies are not interested in information security certification.	There is a need to integrate security strategy as part of the corporate strategy.
[47]	Analysis of security practices and risk assessment in SMEs.	SMEs' lack of adequate attention to IT security, with responsibility frequently unassigned, or allocated to someone without appropriate qualification.	SME security constraints: expertise, awareness and budget require a new risk analysis and management methodology.
[6]	Analysis of the relationship between security policy and strategic information systems plan.	There is no alignment between security policy and strategic information systems plan.	There is a need to specify the alignment between security policy and the strategic information systems plan to guarantee the success of information security.
[45]	Study of the information security strategy and the elements that affect it.	Understanding of information security from a purely technical-technological focus.	Information security should complete the technical-technological focus with business strategy approximations.
[37]	Look at the security measures the small businesses have in place and whether or not they have an information security policy.	The implementation of security policy can be expensive and not feasible for small businesses.	Most SMEs do not have a security policy document, but many are using components that would normally form part of such policy, within their staff employment manuals because it is a much cheaper and less time consuming.

[48]	Raise a holistic approach to facilitate the development of security management systems within SMEs.	The main problems impeding the development of information security within SME: tight budgets, limited human resources, and constantly changing business environments.	The challenges for SMEs can be addressed through a structured methodology that includes four stages: defining security goals of the enterprise, identifying actions, implementing actions and monitoring and reviewing the security implementation.
[7]	They analyze information security with a strategic approximation.	Lack of studies that analyze information security with a strategic and multidisciplinary focus.	A technological focus does not guarantee information security. It is essential to develop an information security strategy aligned to corporate strategy.

In summary, the review of literature indicates the need for an information security strategy at the highest organizational level, integrated into the corporate strategy and, therefore, defined according to the objectives, requirements and context of each company. So, once the strategic importance of information security has been recognized, a policy of information security can be defined for its development as a dynamic process that establishes and monitors compliance of the procedures and specific measures in accordance with the objectives of information security marked by the strategy of the business and the standards and norms that are in application.

3. Methodology of Research

Below, the research methodology used in the work is presented, which is centred on analyzing, using 78 SMEs of the industrial sector, the degree of knowledge that they have of the concept of security policy, what organizational factors limit its application, as well as to analyze its effectiveness with regards to reducing the number of information security problems and its contribution to the generation of value in the business. To do this, a methodology of empirical investigation has been used, supported by techniques of a qualitative nature – group meetings and in depth interviews with company managers – carried out in February and May 2010, and quantitatively – through surveys, data collection and their statistical treatment – developed during the months of January and February 2011.

The choice of the industrial sector was determined because, although its importance is recognized in economics, international organizations describe in their reports that it is a sector

that is falling behind with regard to the implementation of information security measures and which, therefore, needs to improve these levels [40, 49].

As for the type of organizations – SME – as commented in the introduction, it has been considered appropriate to focus this research work on small and medium businesses because, despite the importance that they have in economics [30].there is an absence of works that analyze security in these organizations [33, 34, 49].

Focusing on the companies under study, in the first place it should be noted that they fit the definition of SME established by the European Commission[1] [50], although micro-SMEs, companies with less than ten workers, have been excluded from the study since their small size may influence their investments in technology [28, 51, 42]. As for the number of employees and their qualifications, it should be stated that the companies in the sample have between 10 and 91 employees, with an average number of 26 people on the payroll. With respect to the qualifications of personnel, employees with professional training dominate with 71.4%, followed by those with university degrees which represent 21.16% of the total and a smaller number of non-specialist personnel 7.44%.

Finally, it should be stated that, for the development of the research, two groups were formed; companies with defined security strategies and policies and companies without, taking, having formal information security processes since 2009 as a criterion for classification, two years before the study results, since although there is no consensus in literature as to the exact time period that has to elapse to consider a technology or process consolidated in an organization and which is, therefore, generating effects on the same, theories on the experience and learning effect recommend using periods with delays of between 2 and 5 years [52, 53, 54]. The final result obtained was that 17 companies, 21.79% of the total sample, make up the group of companies with formal information security processes set up by means of an information security policy.

Below, the results divided into two parts are presented; the first part is more descriptive in which the degree of knowledge that companies have about information security is analyzed, how they put it into practice or if not, why not and the second part, in which the analysis of the effects that the application of an information security policy generates is presented.

4. Results and Discussion

4.1 Knowledge and practice of information security in industrial SMEs

There is no doubt that the security policy is a fundamental tool for the development of a security information management system, and thus the different standards and academic and professional Literature gather it [26, 14, 6, 44, 7, 18], but what is not very clear is the

knowledge degree that companies have about this and to know something about it, is the indispensable step to be able to apply it.

In this sense, the first question of interest is to analyze the knowledge degree that companies have about the information security policy concept and what this implies, as well as the company attitude towards these concepts. Secondly, it is interesting to know what elements restrain companies from their application and what organizational aspects distinguish and characterize the companies which apply information security policies from the ones which do not apply them.

For these first questions it must be indicated that information is obtained both interviews in depth and questionnaires passed to the managers and people in charge of the information technology department of the companies of the sample, which later have been processed and put under statistic analysis.

Regarding the first question, the knowledge degree of what information security policy is and implies, as an integrated process in the organization which looks for protecting the information of incidents in a proactive way, and having measures to act in case these happen, knowledge is not very elevated, since only 17 companies, the 21.79%, knew the concept and besides the ones which know it, not all of them apply it, being only 14 companies, the 17.95% of the sample, as companies that systematically apply an information security policy.

Table 2. Concept knowledge and application

	It knows it		**It has being applied it**	
Security policy concept explained and discussed.	**Yes %**	**No %**	**Yes %**	**No %**
	21.79	78.21	17.95	82.05

Before previous ignorance, 78.21% of the managers did not know it, it is interested to see what is the managers' predisposition towards the implantation of security policies once they know the concept and its implications. In such a way that, Table 3 shows how companies once known the concept of information security policy, mainly 54.10% would be interested in implanting and developing it in their organizations.

Table 3. Companies which known the information security policy concept wish to implant it

	Would you be interested in applying it	
Security policy concept explained.	**Yes %**	**No %**
	54.10	45.90

With regard to companies that do not have interest in implanting security policies, the analysis of their rejection is important as it allows to know some factors which restrain from the information security development in companies and therefore the questions on which act to change these behaviors.

Table 4. Reasons for which companies neither apply nor have intention to apply information security policies

Reasons for which do not consider to apply information security policies:	**Frequencies**
It has neither personal nor knowledge to apply it.	11.11%
High cost of application/profits.	55.56%
It considers that is not necessary / do not need it.	33.33%

So that Table 4 shows how companies which do not have interest in developing security policies mainly base their reasoning in which they consider has a high cost 55.56% in relation to the benefit that it generates for the organization. To this degree, it is stated what Literature and the specialized reports have already enumerated as a brake to the investment in information security, the lack of link between this and business variables and indicators that allow to obtain a measure of the obtained yield. Another question that is important to indicate is the such a high number of managers 33.36% do not have interest in information security policies because they consider that they do not need it for their business, which implies not consider the information security as a strategic and dynamic element that evolves in time and in short, they are not giving to information the value that it has.

The latest cause of rejection to the implantation of security policies is, according to managers, not having the sufficient knowledge, which shows the importance of teaching these matters, within the organizations and even in different educative levels especially in University students.

The companies which have no interest in applying security policies were also asked for the business type which they consider needs information security policies, the answers in the group meetings were very varied but after several consensus rounds they took shape in the following.

Table 5. Which organizations it associate with information security policy

	Frequencies
Technological sophistication / high technology companies.	18.31%
Computer science companies.	9.86%
Large companies / high cost.	71.83%

As it can be observed in the Table 5, it prevails the idea of information security is something of large companies and high cost (71.83%). It is very remarkable that 28.17% consider that the information security activities are owned by computer science companies or sectors of high tech.

In this sense, data indicates that the necessity to make aware of information security is a practicable activity in any sector or activity where information and information technologies are used as a part of its business critic activities.

In such a way that Table 6 gathers how companies which neither have security policy nor wish to implant it, have a slanted technological profile of the information security consideration, such as software or hardware tools' possession, looking down the processes and the component of risks' analysis.

Table 6 which tools associate with information security

	Frequencies
Antivirus, firewall, passwords and other technologies.	88.72%
Information processes management.	8.41%
Risk analysis.	4.86%

In order to finalize this descriptive part, companies of the sample split in two groups, with security policy and without it, are asked about a series of questions of organizational type that allow to obtain a profile of the companies which develop security policies, besides analyzing descriptively if those companies have less security incidences, and therefore the information security policy is showed as an efficient process for the information security.

Table 7. Activities linked to the information security which SMEs do - which do not

	Companies with security policies	Companies without security policies
Value from 1 to 7 being 1=really disagreement and 7 really agreement, the following affirmations:	**Average Value**	**Average Value**
The information security is strategic in your company.	6.88	3.12
Your company has a high degree of collaboration with other organizations.	6.17	3.57
The company management and direction are based on economic profile.	3.53	5.81
The knowhow degree of the management is high.	6.37	4.11
The person in charge of the information security is the high direction.	6.48	3.12
The degree of use of IT in the company is high.	5,88	5.81
Last year you have had problems of information integrity: Destruction or corruption of data due to an attack or some other unexpected incident.	2.74	3.86
Last year you have had problems of disclosure of confidential data due to intrusion, pharming, phishing, virus attacks.	2.11	2.98
Last year you have had problems of unavailability of ICT services due to an attack from outside.	2.41	3.10
The number of problems of security originated by the personnel of the organization is high.	1.97	3.15

The results shown by the average values obtained by each group express that for the companies of the sample, the organizations which apply security policies are characterized to have a strategic consideration of the information security, which corresponds with being the high direction the one responsible for these policies. It is emphasized that the management profile is distributed between technicians and managers and it does not seem that this factor has incidence on having security policy, yet the management knowledge degree seems to have it, so that companies which apply information security policies are characterized for having a high technological knowledge management.

Also it is remarkable that the degree of ICT use does not mark giving to information security a strategic importance, nevertheless it seems that when companies work in collaborative surroundings with external organizations, they give more importance to information security.

In conclusion, it seems that cultural factors related to management and its technological knowledge as well as the collaborative context, are those that affect more the strategic consideration of information security.

Regarding the efficacy of having information security policies available, averages clearly indicate that companies with information security policy have suffered fewer incidents, especially highlighting the small number of security problems caused by their own organization's human resources. In consequence it seems to be an appropriate tool for managing information security.

Having presented the results related to the knowledge and application of the information security policies, next the results associated with the analysis of the contribution of information security to the generation of value are displayed.

4.2 Contribution of the information security policy to create value in organizations

One of the conclusions of the group meetings with the persons in charge of companies is that information security leads to a cost of which economic recovery is uncertain, something typical of the intangible resources and assets such as information. In this regard, it should be noted that the activities of valuation of assets and the measurement of its benefits in organizations follow a strict pattern marked by the accounting and the financial economics.

Concerning accounting valuation of information security in organizations, current accounting tools that derive from an industrial economic era -characterized by the tangible capital and assets as essential resources – very different from the current service economy, where information is the main resource, are not valid to reflect the real value generated by the intangible base assets [55, 29, 40]. In fact, accounting has among its fundamental criteria of assets valuation, the depreciation and amortization, which assume a progressive loss in time of the value of an investment for its use and obsolescence.

Something contrary to what happens to the investment in information security, which increases its value by its own characteristics the more its use is, as with this use, the system is refined and improved. For this reason, however accounting standards are required to comply with corporate legislation in each state, are not suitable for the assessment of information security.

In relation to the decision to invest in information security and the measure of its benefits, premiums in general the application of criteria and economic and financial ratios, predominantly among managers and executives the Return On Investment (ROI) and Net Present Value (NPV) of cash flows generated by the investment [56, 57, 58]. These methods basically require the benefits generated by each investment specifically to identify, individualize and quantify monetarily. However, the information security from the business point of view should be considered as infrastructure and support elements for all the activities of the organization where information is involved in [54, 4], this suppose its simultaneous

participation in different business processes that do not need to be related to aspects directly quantifiable in monetary terms.

Consequently, when the nature of the investment and its impressions are as in the case of information security of intangible base, the traditional methods of the selection and evaluation investment present difficulties to be implemented.

In addition, the current dynamics of organizations, in which everything is connected, implies a greater complexity in the definition and representation of the yield variable [28, 51, 40], which needs the evaluation of multiple criteria not only quantitative as profitability and margins on sales, but also qualitative related to intangible processes and assets for its determination [59, 58, 29].

In this way, employers should be aware of the necessity of combining their technological perspective analysis with business processes in their analysis, and in this sense, establish measurement mechanisms that show both the influences of information security has in those essential qualitative processes for its management, and the impact on the economic variables where it can impact on.

As explained in relation to the inadequacy of traditional valuation methods and the complexity of the return variable to measure the impacts on the information security policy business, in this work it was chosen a qualitative and quantitative type of approach, which allowed to know the impression of information security in the elements recognized by the own managers' organizations as critical and distinctive to the organization success. In this particular case, the sample firms identified as key factors for its success, the image and satisfaction that their clients and the internal processes of the organization have, difficult economic quantifying aspects, but without a doubt they have a bearing on the results of organizations.

Furthermore, given by definition the information security improve the organization information system and, in that event communication and coordination, according to the managers' opinion it was selected, as variables of economic and financial kind on which the information security affect, the coordination and productivity costs of the company.

Regarding the investigation procedure used, to each critical factors selected by the managers, customer satisfaction and internal processes, indicators were developed by likert[2] scales. Once collected the indicators, to each one of them, analysis of variance models (ANOVA[3]) were generated, that after the division of the sample firms into two groups −with information security policies in operation and without them− make possible to ascertain the significant existence of statistically impacts between the use of a security policy (independent variable of contrasts) and the scales of each one of the factors (dependent variables of contrasts).

In the following section the results of each of the key factors are listed and discussed by means of tables which show, for each group of companies and in each indicator of the scale, the average values, the statistic F value of Snedecor[4] and the contrast significance[5].

4.2.1 Security policy effect on client satisfaction

The study of the effect of using a security policy on the dependent variable of the client satisfaction is performed by different ANOVA models, one for each of the attributes that make the assessment of the client.

Table 8. Scale formed as an indicator of client satisfaction

Attribute	**How you believe customers value your company in comparison with competitors in the following aspects** being 1= the worse and 7= the better							
SC1	Security in the commercial information exchange	1	2	3	4	5	6	7
SC2	Security and tracking of orders and payments' information.	1	2	3	4	5	6	7
SC3	Security and confidentiality in customer service.	1	2	3	4	5	6	7

Table 9. Security and satisfaction policy of the client

Security policy	**(Averages) SC1**		**SC2**	**SC3**
SI	6.16		6.84	5.46
NO	3.75		3.21	3.12
	F Value	9.25	15.37	8.47
	Significance	0.007*	0.001*	0.009*

As it is observed in Table 8 and 9, the results of the average values and the contrast significance show the obtaining of a positive impact for the three attributes. This allows the companies of the sample to confirm the existence of a positive relation between the use of a security policy and the achievement of better results in the valuation that clients' managers perceive towards their company. The explanation seems clear, the companies value positively work with other organizations which can guarantee the security on the information which they share and the confidentiality in transactions.

4.2.2 Security policy effect on the internal processes of the organization

In the industrial companies the internal processes are very important and require a high degree of synchronization to avoid productive process inefficiencies and ruptures. In

consequence, it is interesting to analyze if the company's security policy with respect to the protection, availability and integrity of the information, affects these processes.

Table 10. Scale formed as internal processes indicator

Attribute	**How you think clients value your company in comparison with the competition in the following aspects** being 1= the worse and 7= the better							
SP1	The number of stock ruptures (has decreased).	1	2	3	4	5	6	7
SP2	The number of problems in the productive processes by information problems (has decreased).	1	2	3	4	5	6	7
SP3	The number of times that has failed to fulfill the delivery deadline by information problems (has decreased).	1	2	3	4	5	6	7

Table 11. Results of the ANOVA security policy and attributes of internal processes

Security policy	**(Averages) SP1**		**SP2**	**SP3**
SI	5.76		5.84	5.66
NO	3.25		2.91	3.12
	F Value	9.15	13.37	9.27
	Significance	0.007*	0.001*	0.007*

In the Table 11 it is observed how the companies that have the information security policy obtain a better average behavior in each one of the attributes, this jointed with the contrast significance, indicate that the companies of the sample that have information security policy have had smaller problems in its internal processes. So that companies with different effort levels in information systems and IT hold as well, different operation and economic yield results, being the most positive variations in the companies that present major stress in IT. Accordingly, for the companies of the sample it is verified that exists a positive influence of the efforts in IT on the achievement of the better results in the financial perspective.

4.2.3 Effect of the information security policy in the coordination costs and productivity of the organization

Finally, analyzed the facts of having information security policy on the areas of more qualitative character of value creation – client satisfaction, internal processes – it is proceeded to study the existence of statistical forces between having information security policy and the financial perspective of the company, represented by the indicators: internal coordination

costs (defined as costs which the company falls into in its normal running) and productivity (defined as total cost of production/amount of sales).

The fruit analysis on the internal coordination costs and productivity is realized by means of ANOVA models, in which the independent variable represents two groups; the first formed by the companies that possess information security policy and the second by the companies which do not have that policy, and as a dependent variable the manager's perception of the evolution of the internal coordination costs and the productivity of the organization.

Table 12. Information security policy effect in the coordination and productivity costs

Security policy	**"Increase of last year coordination costs" Average**		**"Increase of last year productivity" Average**
SI	2.07		3.82
NO	3.62		3.09
	F Value	5.723	4.123
	Significance	0.001	0.018

As it is observed in Table 12, for the coordination costs the results of the averages and the contrast significance highlight the existence of a positive relation between having information security policy and the internal coordination costs, so that the companies with information security policy show a more favorable evolution of its coordination costs. With regard to the productivity, averages indicate that the group formed by the companies with information security policies have improved its productivity more, although statistical significance has not been reached, possibly because the reduced sample size causes that the differences between the averages of the groups are very high and for the productivity case there are differences even though they are not excessive.

Conclusions

The development of information society and the possibilities offered by the continuous technological development have resulted in a digitalization without precedents of business environment, in which the daily life of organizations and their business processes – customer relations, production, procurement, billing and payments, and so on – depend on their ability to manage information. Hence information has become a valuable strategic asset for organizations, which protection and security should also acquire this strategic consideration.

The academic literature, professional reports and official statistics relating to information security in organizations, reveal the existence of two important gaps: first, the excessive focus on technology from which are analyzed, studied and put into operation the information security, and second, the need to extend the analysis, studies and policies on information

security to small and medium enterprises, because despite their importance in the economies, have lagged behind in matters relating to information security, compared to large companies.

In this regard, in recent years have seen an evolution in research on information security to the consideration of organizational variables and how they affect the fulfillment of standards and information security management models. Also in recent years have developed studies analyzing the relationship between information security and financial performance variables and image of businesses. However, recent literature emphasizes that the complexity and interdisciplinary nature of information security, makes it necessary further analysis through complementary approaches, technological and business, that bring information security to the questions that concern to managers of companies: customer satisfaction, its contribution to internal processes and productivity, and ultimately their contribution to generation of value for the company.

In the same line, the professional reports highlight that one of the causes of the low regard of information security at the strategic level in organizations is the lack of understanding between technology and business variables.

Is in this context in which the policy of information security has a key role as a dynamic process, participatory and organized that has to serves as nexus between business strategies and technological strategies of the organization. In this sense, the policy of information security becomes in the driving element for the planned establishment of measures, action protocols and controls – which affect the processes, technology and people – aimed at protect the information according to the needs of the strategy and compliance with standards and legislation.

From the foregoing considerations an investigation was developed in 78 industrial SMEs with two major objectives. First, determine the degree of knowledge that companies have of the concept and implications of the security policy information, analyze their attitude towards such concept and in this sense establish what questions incise as brakes to their development, what characterize the companies it apply and if security policies are effective and reduce the incidents of information security in companies. Second, analyze whether the information security through the establishment of a security policy, contributes to the generation of value for the business.

Regarding the first objective, of the analysis we can conclude that the degree of knowledge and application in the companies of the security policy is low, although it should be noted that once companies know what is the security policy information and its implications, mostly show interest in its developing in their organizations.

Regarding the elements that act as brakes, notes that information security is still considered by managers as an expense and not as an investment, this is due to lack of knowledge that allows them to measure, in their own business language, how information security affects the business variables and thus obtain a measure of its profitability. Furthermore, it should influence on the disclosure and awareness of the importance of information security, since a large number of companies believe that the policy of information security is not interested because it does not affects them, reflecting that in their opinion is a subject of large companies and technology companies. In this sense, the companies that have not interest in establishing policies for information security stand out by having a vision of information security with a biased technological profile, limited to the possession of software tools or hardware, neglecting the component of risks analysis and processes associated with information security.

With regard to some of the organizational characteristics that may influence a company has a strategic consideration of information security, rather than the profile of managers, which has a favorable impact is that they have a high degree of knowledge about information technologies. Moreover, does not affect the level of use that companies make ICT but for that they use them. In addition, working in collaborative environments with outside organizations affects positively in the strategic consideration of information security.

Respect to the effectiveness of dispose of information security policies, it confirms its usefulness because the companies that have information security policy have suffered less incidents, acting in manner especially effective in reducing security problems caused by themselves human resources of the organization.

As regards the second objective of our study, analyze whether the information security, through the establishment of a security policy, contributes to the generation of value for the business. It should be noted that given the difficulty of measure the benefits from intangible assets, that are synergistic and affect the entire organization, we opt to develop indicators of qualitative type that will be able to measure results on process type variables, which themselves managers had considered critical for their business – customers and internal processes – and combine it with indicators of more quantitative type – costs of coordination and productivity –.

It is this sense we can conclude that information security as a process developed through a security policy, contributes both to improve the protection of information and reduce the number of incidents, as the generation of value, because they improve the customer satisfaction with the company, recognizing it as being safer; improve internal processes

avoiding interruptions in the production system due to failures in the information, and helps to reduce the coordination costs and enhance productivity of companies.

Finally, we must not forget that this work has focused on 78 SME of industrial sector and although the research results presented here are significant for the sample companies, these should be considered carefully in terms of extrapolation and generalization to the whole of industrial enterprises. In this sense, as a future line of work will be very interesting extend the number of companies of the sample and replicate this work in other sectors such as service companies.

Acknowledgements

This paper has been possible thanks to the financing and support for the research provided by the National Plan of R+D and the Interministerial Commission of Science and Technology, Government of Spain, (Research Project: DPI2002-04342-C05-03), and the collaboration of managers and directors of the companies.

Notes

[1] Definition established by the European Commission (DOCE 20.05.2003) official from January 1, 2005, summarized below:
Micro enterprise: less than 10 employees and a limit of 2 million euros to the turnover and the balance sheet.
Small enterprise: 10 to 49 employees. The limit of turnover and balance sheet is 10 million euros.
Medium enterprises: 50 to 249 employees. The limit of turnover will be up to 50 million euros and the balance sheet, up to 43 million euros.

[2] Statistic instrument of ordinal measurement consisting of a series of items or judgments, concerning to the same concept, for which seeks the opinion of the respondent. The usefulness of these tools is which permit the measurement of attitudes and behaviors.

[3] Statistical models of variance analysis, that allow check the explanatory power of a factor, independent variable of categorical type, on a dependent variable of metric character. The ANOVA techniques are used to contrast the statistical significance of means differences between groups or levels of the independent variable and allow establish statistically the existence of relationships between variables, as well as the direction or effect which takes such relationship [60].

[4] Statistical that allow check the existence of statistically significant differences in the variances of two normal populations.

[5] The relationships are statistically significant based on the value taken by the significance, also called "p-value." When the significance value of is less than 0.10 the relationship is statistically significant at a confidence level of 90%. Being the most favorable a confidence level as high as possible, of 95% when the significance is less than 0.05 and 99% when takes value less than 0.01.

References

[1] Nolan, R. L., *Information technology management from 1960-2000*. Harvard Business School, Boston, 2001.

[2] Drucker, P. F., *Managing in the next society*. St. Martin Press, New York, 2002.

[3] Gordon, L. A. and Loeb, M. P., Economic aspects of information security: an emerging field of research. *Information Systems Frontiers*, 8:5 (2006), 335-337.

[4] Preston, D. S. and Karahanna, E., Antecedents of IS strategic alignment: a nomological network. *Information Systems Research*, 20:2 (2009), 159-179.

[5] May, C., Dynamic corporate culture lies at the heart of effective security strategy, Computer Fraud & Security, 2003:5 (2003), pp.10–13.

[6] Doherty, N.F. and Fulford, H. Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 25:1(2005).55–63.

[7] Park, S. and Ruighaver, T. Strategic approach to information security in organizations, *in Proceedings of the 2008 International Conference on Information Science and Security*. (2008).

[8] *The promotion of a culture of security for information systems and networks in OECD countries*. OECD, 2005.

[9] *The availability, reliability and security of networks and information systems are increasingly central to our economies and to the fabric of society*. Commission of the European Communities. COM, 2006.

[10] Pérez, D. and Solana, P., Intranets: medición y valoración de sus beneficios en las organizaciones. *El Profesional de la Información*, 15:5 (2006), 331-341.

[11] Kannan, K. and Telang, R., Market for software vulnerabilities? Think again. *Management Science*, 51:5 (2005), 726-740.

[12] Luftman, J. and Ben-Zvi, T., Key issues for IT executives: difficult economy's impact on IT. *MIS Quarterly Executive*, 9:1 (2010), 49-59.

[13] Kim, S., Leem, C. S. and Lee, H. J., An evaluation methodology of enterprise security

management systems. *International Journal of Operations and Quantitative Management*, 11:4 (2005), 303-312.

[14] ISO/IEC 27001, *Information technology, security techniques, information security management systems: requirements*. International Standard Organization, 2007.

[15] Kwon, S., Jang, S., Lee, J. and Kim, S., Common defects in information security management system of Korean companies. *Journal of Systems and Software*, 80:10 (2007), 1631-1638.

[16] Siponen, M. and Willison, R., Information security management standards: problems and solutions. *Information & Management*, 46:5 (2009), 267-270.

[17] Smith, S. and Jamieson, R., Determining key factors in e-government information system security. *Information Systems Management*, 23:2 (2006), 23-32.

[18] Solana, P. and Pérez, D., Security model applied to electronic records management: experiences and results in the nuclear sector. *International Journal of Technology Management*, 54:2/3 (2011), 204-228.

[19] Garber, L., Denial-of-service attacks rip the internet. *IEEE Computer*, 33:4 (2000), 12-17.

[20] Hawkins, S., Yen, D. C. and Chou, D. C., Awareness and challenges of Internet security. *Information Management & Computer Security*, 8:3 (2000), 131-143.

[21] Liu, W., Tanaka, H. and Matsuura, K., *An empirical analysis of security investment in countermeasures based on an enterprise survey in Japan*. Fifth Workshop on the Economics of Information Security (WEIS), 2006.

[22] Kim, S. and Lee, H. J., Cost-benefit analysis of security investments: methodology and case study. *Lecture Notes in Computer Science*, 3482 (2005), 305-315.

[23] Cavusoglu, H., Mishra, B. and Raghunathan, S., The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9:1 (2004), pp. 69-104.

[24] Campbell, K., Gordon, L. A. Loeb, M. P. and Zhou, L., The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11:3 (2003), 431-448.

[25] Dhillon, G. and Backhouse, J., Information system security management in the new millennium. *Communications of the ACM*, 43:7 (2000), 125-128.

[26] BS7799-2, *Specification for information security management systems*. British Standard Institute, London, UK, 2002.

[27] Navarro, M., Security evolves towards maturity. *Universia Business Review*, 2nd quarter, 10 (2006), 96-103.

[28] Melville, N., Kraemer, K. and Gurbaxani, V., Review: information technology and organizational performance: an integrative model of IT business value. *MIS Quarterly*, 28:2 (2004), 283-322.

[29] Hubbard, D. W., *How to measure anything: finding the value of intangibles in business*. 2nd Edition. Wiley, 2010.

[30] *The impact of the global crisis on SME and entrepreneurship financing and policy responses*. OECD, 2009.
http://www.oecd.org/dataoecd/40/34/43183090.pdf

[31] Luftman, J. and Ben-Zvi, T., Key issues for IT executives 2010: judicious IT investments continue post-recession. *MIS Quarterly Executive*, 9:4 (2010).

[32] *Findings from the 2011 global state of information security survey*. PricewaterhouseCoopers, CIO Magazine and CSO Magazine, 2011.
http://www.pwc.com/gx/en/forensic-accounting-dispute-consulting-services/state-information-security-survey-2010.jhtml

[33] Kraemer, S., Carayon, P. and Clem, J., Human and organizational factors in computer and information security: pathways to vulnerabilities. *Computers & Security*, 28:7 (2009), 509-520.

[34] Pritchard, S., Navigating the black hole of small business security. *Infosecurity*, 7:5 (2010), 18-21.

[35] Directorio Central de Empresas (DIRCE), 2010.

[36] *Information technology security handbook*. World Bank, 2003. ISBN 0-9747888-0-5.

[37] Burns, A., Davies A. J. and Beynon-Davies, P., A study of the uptake of information security policies by small and medium sized businesses in Wales. *ICEB & eBRF 2006 Conference*. Tampere, Finland, 2006.

[38] Sánchez, L. E., Santos-Olmo, A., Fernández-Medina, E. and Piattini, M., Managing security and its maturity in small and medium-sized enterprises. *Journal of Universal Computer Science* (J.UCS), 15:15 (2009), 3038-3058.

[39] Dhillon, G. and Backhouse, J., Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11:2 (2001), 127-153.

[40] Giannakouris, K. and Smihily, M., *ICT security in enterprices, 2010*. Eurostat, European Commision, 2010.

[41] Luftman, J., Kempaiah, R. and Nash, E., Key issues for IT executives. *MIS Quarterly Executive*, 5:2 (2006), 81-101.

[42] May, J., and Dhillon, G., *A holistic approach for enriching information security analysis and security policy formation*. ECIS 2010 Proceedings, Paper 146. http://aisel.aisnet.org/ecis2010/146

[43] Ward, J. and Peppard, J. Strategic Planning for Information Systems, John Wiley & Sons (2002).

[44] Von Solms, B. and Von Solms, R. 'From information security to business security' Computers & Security, 24: 4(2005), pp.271–273.

[45] Wang, G. Strategies and influence for information security. *Information Systems Audit and Control Association*, 1, (2005)

[46] Hone, K. and Eloff, J.H.P. Information security policy – what do international security standards say? *Computers & Security*, 21: 5(2002), pp.402–409.

[47] Dimopoulos, V., Furnell, S.M., Jennex, M. and Kritharas, I., Approaches to IT security in small and medium enterprises. *Proceedings of the 2nd Australian Information Security Management Conference 2004*. Perth, Australia, 2004.

[48] Tawileh, A., Hilton, J. and McIntosh, S., Managing information security in small and medium sized enterprises: a holistic approach. *Proceedings of the ISSE/SECURE 2007 Securing Electronic Business Processes*, 2007, pp. 331-339.

[49] OECD, Information Technology Outlook 2010. OECD, (2010) ISBN 978-92-64-08873-3

[50] European Commission (DOCE 20.05.2003)
http://europa.eu/legislation_summaries/enterprise/business_environment/n26026_es.htm

[51] Liu, Y. and Ravichandran, T., A comprehensive investigation on the relationship between information technology investments and firm diversification. *Information Technology and Management*, 9:3 (2008), 169-180.

[52] Powell, T. C. and Dent-Micallef, A., Information technology as competitive advantage: the role of human, business, and technology resources. *Strategic Management Journal*, 18:5 (1997), 375-405.

[53] Brynjolfsson, E. and Hitt, L. M., Computing productivity: firm level evidence. *Review of Economics and Statistics*, 85:4 (2003), 793-808.

[54] Lee, J. J.-Y., Complementary effects of information technology investment on firm profitability: the functional forms of the complementarities. *Information Systems Management*, 25:4 (2008), 364-371.

[55] Lev, B., *Intangibles: management, measurement, and reporting*. Brookings Institution Press, Washington, D.C., 2001, ISBN 0-8157-0094-6.

[56] Mahmood, M. A. and Mann, G. J., Measuring the organizational impact of information technology investment: an exploratory study. *Journal of Management Information Systems*, 10:1 (1993), 97-122.

[57] Im, K. S, Dow, K. E. and Grover, V., Research report: a reexamination of IT investment and the market value of the firm-an event study methodology. *Information Systems Research*, 12:1 (2001), 103-117.

[58] Chen, Y., Liang, L., Yang, F. and Zhu, J., Evaluation of information technology investment: a data envelopment analysis approach. *Computers and Operations Research*, 33:5 (2006), 1368-1379.

[59] Sher, P. and Lee, V. C., Information technology as a facilitator for enhancing dynamic capabilities through knowledge management. *Information and Management*, 41:8 (2004), 933-945.

[60] Hair, J. F., Anderson, R. E., Tatham, R. L. and Black, W. C., *Análisis Multivariante.* 5ª Ed. Prentice Hall. Madrid, 1999. ISBN 8483220350.

Biographical Notes:

Daniel Pérez González received his Ph.D. in Business Administration from the University of Cantabria and he is currently Professor of Information Systems in the Faculty of Business and Economics (UC) since 2001 and member of the Information Management RD&I Group. He is also a member of The European Academy of Management and Business Economics and invited Lecturer in the Institute for Market Research of Kiel (Germany). He has participated in public projects of the Spanish Inter-ministerial Commission of Science and Technology (CICYT) and has been Chair in various international conferences and published several articles in technology and business journals.

Pedro Solana González is a Computer Engineer in Polytechnic University of Catalonia with a Postgraduate in Computer Science and Ph.D. in Industrial Engineering from the University of Cantabria (UC). He is Professor of Information Systems in the Faculty of Business and Economics (UC) since 1995 and member of the Information Management RD&I Group. He is also a Director of different investigation projects about document management, security management, innovation and processes improvement (2000–2008). He has participated in public projects of the Spanish Inter-ministerial Commission of Science and Technology (CICYT) and has been a reviewer in various international conferences.

Sara Trigueros Preciado is an Industrial Technical Engineer with a Postgraduate in Business and Information Technology from the University of Cantabria (UC). She has been a professor of technology in academic centers and has participated in several conferences and academic publications. Nowadays, she works in innovation, technology and product development in a multinational organization.

***Corresponding author:** Daniel Pérez González, Ph.D.
Department of Business Administration,
University of Cantabria,
Avda. Los Castros s/n. 39005 Santander, Spain
E-mail: daniel.perez@unican.es