Advances in Intelligent Systems and Computing 353

Álvaro Rocha
Ana Maria Correia
Sandra Costanzo
Luís Paulo Reis Editors

New Contributions in Information Systems and Technologies

Volume 1

Springer

Implementation of Information Systems Security Policies: A Survey in Small and Medium Sized Enterprises

Isabel Lopes and Pedro Oliveira

School of Technology and Management, Polytechnic Institute of Bragança, Portugal
{isalopes,pedrooli}@ipb.pt

Abstract. Information has become organizations' most valuable asset, thus being a potential target to threats intending to explore their vulnerabilities and cause considerable damage. Therefore, there is a need to implement policies regarding information systems security (ISS) in an attempt to reduce the chances of fraud or information loss. Thus, it is important to find the critical success factors to the implementation of a security policy as well as to assess the level of importance of each one of them. This paper contributes to the identification of such factors by presenting the results of a survey regarding information systems security policies in small and medium sized enterprises (SME). We discuss the results in the light of a literature framework and identify future works aiming to enhance information security in organizations.

Keywords: Information Security, Information Systems Security Policies, Small and Medium Sized Enterprises.

1 Introduction

The massification of computer use as well as the vast internet use within organizations has brought about an increasing exposure of information. SMEs are also being affected by this problem but have fewer resources available to intervene in the management of information security.

According to [1], information is an asset which, like any other asset, is important and essential to an organization's business, and must, therefore, be appropriately protected. Information is currently seen as one of the most important resources within an organization, giving a decisive contribution to its higher or lower competitiveness.

In the view of [2] and [3], information security must be understood within the organization's context of culture, policies, organizational structures and operating environment used in order to ensure the integrity, availability and confidentiality of its information.

The word security is associated with risks as well as with their prevention and minimization. Therefore, it is necessary to take preventive measures which, if not sufficiently capable of avoiding undesirable, malicious or unpredictable occurrences, may at least predict actions to be taken in order to minimize such occurrences.

Information is an asset which must be protected and cared for by the means of rules and procedures described in a security policy.

Á. Rocha et al. (eds.), *New Contributions in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 353, DOI: 10.1007/978-3-319-16486-1_45

The ISS policy sets rules and standards of conduct with the aim to determine the probability of occurrence of incidents which may cause, for example, service unavailability and information theft or even loss.

ISS policies consist essentially of documents which guide or regulate the actions of people or systems within the ISS domain [4]. Information systems security policies are pointed out in literature as one of the main measures to be taken by organizations for protecting their information systems.

The research question discussed in this work is: Which factors can influence the implementation of an ISS policy in a SME?.

The aim of this study was to identify the critical success factors to the implementation of an ISS policy in a SME and to assess the level of importance of each one of those factors.

The structure of the paper is as follows. After this introduction, we proceed with a review of literature on information security and relevant terms. Afterwards, in section 3, we focus on what is meant by ISS policy implementation. In section 4, we describe the research methodology. The results of the study are discussed in section 5. In the last section, we present conclusions in the light of the results and propose future works.

2 The Importance of Information Security

Due to the massive use of Internet as well as to the constant growth in the use of technological means by SMEs, information is increasingly exposed to threats. Therefore, information security plays an essential role to ensure the integrity, confidentiality and availability of these assets.

The CIA triad – Confidentiality, Integrity and Availability – represents the conventional properties which guide the analysis, planning and implementation of information security. Other properties such as legitimacy and authenticity are emerging because of the widespread of the use of commercial transactions through computer networks worldwide.

The classic principles of CIA can be explained as follows:

- Confidentiality – access to information restricted to legitimate entities, that is to say those authorized by the information owner.
- Integrity – manipulated information must preserve all the original features established by the information owner, ensuring that the content is not altered without permission.
- Availability – the information is available for legitimate use at all times, whenever necessary.

These principles are considered traditional for the authors [5], who claim that they are good as long as they serve their purpose, but who find them very restrictive and applicable mainly to the information viewed as data kept in computer systems. Therefore, these authors add other principles without which future organizations may face serious problems. These new principles were condensed in the acronym RITE – Responsibility, Integrity, Trust and Ethicality – and they are viewed by the authors as instrumentals for the creation of an information security culture within organizations in a near future.

RITE principles can be explained as follows:

- Responsibility – It gains importance as organizations are abandoning the vertical/hierarchic organizational structure.
- Integrity – Dealing with valuable information without revealing it or giving in to pressures.
- Trust – Higher self-control and responsibility at the expense of external control and supervision.
- Ethicality – Ethics must be present in all informal, new and dynamic situations in order to enhance an appropriate response from cooperators when faced with those new situations.

Information is an asset which, like any other asset, is important for business and valuable for the organization, thus needing adequate protection.

Information security protects information from several types of threat in order to ensure business continuity, minimize damage and maximize both return on investments and business opportunities [6].

In order to reach this level of protection, companies must stop worrying only about crackers' attacks or about the implementation of firewalls and/or anti-viruses. They must start focusing their attention on the creation of an actual information security culture, which includes the measures mentioned above, but with a wider scope and a higher degree of efficiency. For [7], setting a firewall does not alone ensure the security of internet access. Therefore, according to this author, a set of other considerations must be established, such as policies, procedures, norms and other management instructions.

3 Implementation of Information Systems Security Policies

In order to achieve information security, it is necessary to implement a set of adequate measures aiming to ensure the security of that asset. One of the measures consists of creating a set of norms and recommendations usually written in a document called ISS policy.

The creation of an ISS policy follows a complete life cycle from its drafting to its implementation and review. This study focuses on the implementation of a policy, which can be considered as a set of activities which aim to prescribe what is written in the policy document.

There are six main principles to be considered within the process of implementing an ISS policy [8]:

1. The organization will ensure that its information is kept safe and used in an appropriate way;
2. The organization will provide clear guidance to human resources regarding information security;
3. All human resources working for and on the behalf of the organization will cooperate with the information security policy within the organization;

4. The organization will ensure that its human resources know all the relevant guidelines regarding the organization's information security;
5. The organization will inform its clients about the way their records will be kept safe as well as of who will have access to them;
6. The organization will comply with all the national legislation as well as with the best guidance regarding information security.

In figure 1, we present a process of ISS policy implementation [9]. This process includes input elements which feed certain activity processes which, in turn, will originate a set of outputs.

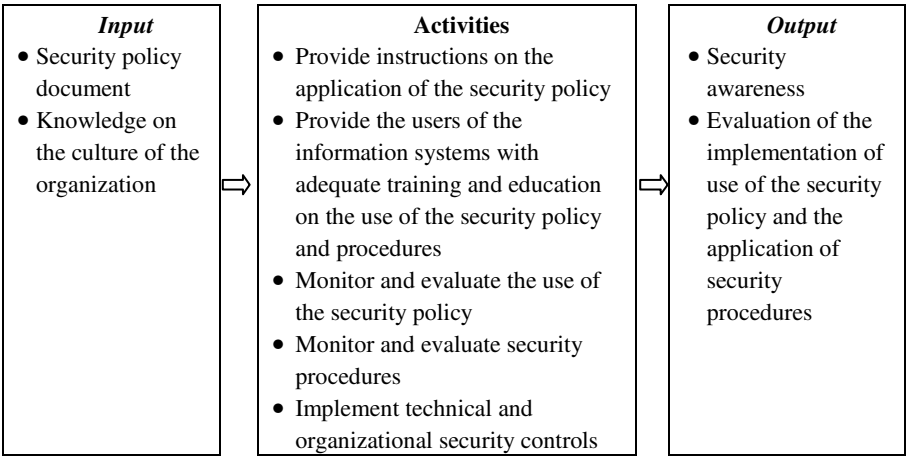

Fig. 1. The process of security policy implementation

This process ultimately results in the implementation and subsequent conscientiousness of both users and managers regarding the obligation of using the policy with utmost rigor and seriousness.

The input of the ISS policy implementation process includes not only the policy document but also the knowledge and relevant information regarding the organization's social and cultural aspects. Among the activities which are to be developed from those inputs, we highlight the following: training and education of the policy users concerning the adequate application, procedures and use of the policy. After these steps are taken, they are to be monitored and assessed [10].

4 Research Methodology

In order to characterize empirically the adoption of an information security culture by the Portuguese SMEs, the most appropriate applicable technique was found to be the Survey, as it enables a clear, direct and objective answer to the questions presented to

the respondents. Besides this, as the universe under study comprises about 248,552 companies, among which 350 were surveyed, we thought that this number undermined the adoption of alternative research techniques.

Considering the fact that the survey addressed SMEs, it is essential to define this latter concept. The status of SME (Small and Medium sized Enterprise) is defined in the Decree-Law n. 272/2007 of November 6, according to the companies' number of permanent workers, which must be under 250; the turnover, which must be under or equal to 50 million Euros; and an annual balance-sheet total which must be under or equal to 43 million Euros.

The selection of the companies surveyed in this study was made considering the geographical area and the number of workers. In Table 1, we present the number of workers and their representativeness within Portuguese business.

Table 1. Number of workers and percentage in 2012 in Portugal

Type of Enterprise	N. of Workers	Percentage
Micro	1-9	94.6
Small	10-49	4.7
Medium sized	50-249	0.7
SME= 1+2+3	1-249	99.8

As shown in the above table, SMEs in Portugal represent 99.8% of business. Their representativeness is extremely high, which makes them deserve more attention in many respects.

4.1 Population

Among the 348,552 SMEs which represented the target of the survey under analysis, 350 questionnaires were conducted. However, only 307 obtained an effective response, which corresponds to an 88% answer rate. The selection was made through a random sampling based on the number of workers and on the scope of the 18 districts in Portugal plus those of Madeira and Azores.

Among the answers obtained in the 307 contacts established, 288 were obtained by telephone and 19 via email after a previous telephone contact.

An effort was made to ensure that, in the highest possible number of cases, the respondent to the survey would be the person in charge for the IT sector.

The study was conducted between September and October 2013.

4.2 Structure

The structure of the survey resulted from the review of literature on information security. It had a comprehensive cover, although the focus for this study was given to the critical success factors to the implementation of an ISS policy and to their level of importance.

The questions of the survey were of individual and confidential answer, and they were organized in three groups.

The first group aimed to obtain a brief characterization of the company and of the respondent. The other two groups contained questions concerning the information security culture, with a first main question: "Does the company have an information security culture?"

When the answer to that main question was negative, the next step consisted of answering the group of questions concerning the possible adoption of an information security culture. The respondents were asked whether they intended to adopt any measures and behavior which might contribute for the company to have an information security culture, and if so, whether such measures were already being prepared or not. If they were not planning to adopt any measure, the respondents were asked whether such option was being made for not considering information security an important issue.

When the answer to the main question was positive, the respondents would proceed to answer the groups of questions focusing on the type of measures adopted, and were asked to list relevant enabling and inhibiting factors regarding the adoption of such measures as well as the level of importance of each of those factors.

One last question was asked to the respondents, which regarded the existence and identification of other information protection mechanisms.

5 Results

This study was carried out between September and October 2013. During this period of time, 350 companies were contacted by phone and among these, 307 responded to the survey.

As shown in Chart 2, among the respondents, 57% were head of the IT department, 22% were partners or owners of the company, 15% were supervisors and the remaining 6% were administrative officers.

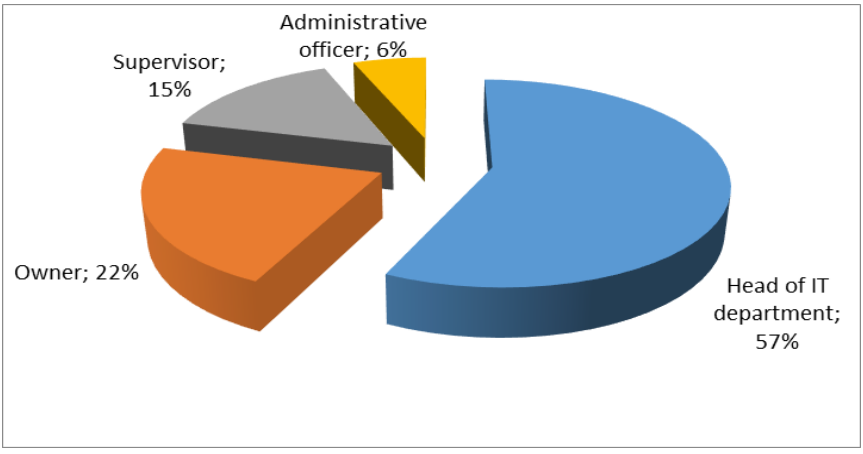

Fig. 2. Distribution of the respondents' position in the companies

As far as the 307 SMEs characteristics are concerned, Chart 3 shows the results regarding the types of company: 100 are Micro enterprises (up to 9 workers); 90 are Small enterprises (between 10 and 49 workers); and 117 are Medium sized enterprises (between 50 and 249 workers). An effort was made to ensure that the number of the different company types and their geographic distribution would be as analogous as possible.

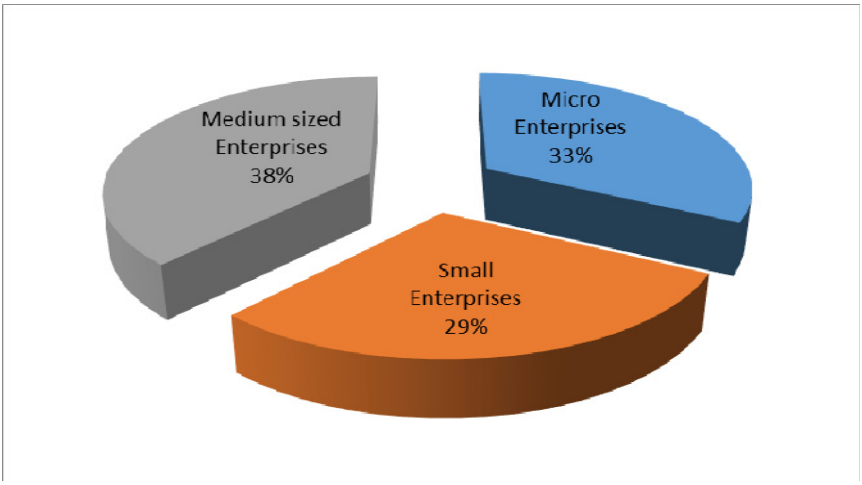

Fig. 3. Distribution of the type of company surveyed

The most relevant question of the survey for this study regarded the identification of the critical success factors to the implementation of an ISS policy. We must point out that among the 307 SMEs, 29 (9%) reported to have an actual information security culture and 278 (91%) have some measures adopted, but these are not relevant enough to enable them to say that they actually have an information security culture.

The disparity of these figures made it even more relevant to find out which key-points are observed in the implementation of an ISS policy. Such points are presented in the following paragraphs.

The success of a policy highly depends on its users' compliance. Although the ISS policy guidelines are prescriptive and therefore compulsory to its users, it has been observed that the latter frequently fail to comply with the rules [11].

Another critical factor to the implementation of an ISS policy is the willingness of the executive board throughout the process. A good drafting, implementation and adoption of an ISS policy can only be achieved with the involvement of all the organization's cooperators and especially that of its head offices.

An ISS policy is usually targeted towards a diverse audience, to whom information security may represent a new and strange concept. Therefore, it is essential that users know and understand the definition of information security and that this understanding and definition are uniform within the organization.

Another factor that was mentioned as essential to the success of the policies is the engagement in the policy implementation, especially with regard to its communication and dissemination among those who must know and observe it.

Indeed, all the organizational stakeholders must know about the security policy. The dissemination means may vary from posting the policy to making it available on the SME Intranet or by other means, but it is crucial to ensure that everyone has been notified of the content of the policy.

The existence of a rolling plan regarding users' training and education in the domain of ISS, as well as the assessment of the security policy efficiency both contribute to the successful implementation of the information security policy.

Another factor mentioned concerned the document features. The policy must be understood, therefore, it cannot be too long, it must be correctly structured and be written in a simple style. A policy whose understanding and feasibility turn out to be impossible will be of little or no value to the organization.

Approval from superiors was also referred to as a key-factor to a more effective implementation. This additional sign of commitment from the executive board towards information security has an effect on the acceptance of the policy by its users.

Users' resilience to change usually inhibits the implementation of an ISS policy. Therefore, in order to overcome this obstacle, users must understand the advantages of information security and have a positive view on the changes which their daily working procedures will undergo by implementing the ISS policy.

Technology is another aspect pointed out as a basic support tool to information security, as although technology and the policy document are distinctive, they are complementary. Therefore, having good technologies within the SME will be of little use if the set of norms and procedures regarding information security is not implemented. Similarly, having an excellent document will be useless if there are no technological means such as anti-viruses and firewalls to complement it.

Due to the big difference observed between the SMEs which have an information security culture and those which do not, we analyzed the level of importance of each critical success factor to the implementation of an ISS policy separately, as shown in Table 2. The SMEs which have a security culture were named Cluster 1 and those which belong to the group where there is no security culture were named Cluster 2.

The level of importance of critical success factors to implement an ISS policy, beyond being split in Clusters, to its quantification, were considered how many times those factors were mentioned by the inquired enterprises: 29 belonging to Cluster 1 e 278 belonging to Cluster 2.

Table 2. Level of importance of critical success factors

Cluster 1	N.	Cluster 2	N.
Users' training	8	Executive board willingness	64
Compliance monitoring	6	Users' training	60
It has the Executive board approval	5	Users' understanding	45
Users' compliance	3	Engagement in implementation	39
The document is not long	3	Compliance monitoring	36
The document is clear and concise	2	Acquisition of technologies	22
Engagement in implementation	1	Defining goals	12
Defining the policy	1		

The analysis of the two clusters shows that the factor users' training has considerable weight in both cases. In cluster 1, the level of importance focuses more on the document and its characteristics, whereas in cluster 2, as such a document does not exist in most cases, more focus is given to the executive board willingness to implement an ISS policy as well as to the users' understanding the advantages of such implementation. Engagement in the implementation of the policy is more valued in cluster 2, and so is the importance given to technology and IT equipment, which is not even mentioned in cluster 1.

6 Conclusion

The study presented was based on a survey conducted among 350 SMEs in Portugal, from which 307 responded to the survey, thus obtaining a response rate of 88%. This study identified a set of critical success factors to the implementation of an ISS policy as well as the level of importance of such factors.

The implementation of an ISS policy is a dynamic process that must include a regular sub-cycle during which the policy is assessed, planned and corrected. These sub-cycles are justified by the existence of variables such as experience, implementation problems, limitations and technological developments which, if not taken into account, may turn the policy into an inoperative and utopic document [10].

We hope that this work can represent a positive contribution to SMEs. Although it is impossible to ensure that companies will be totally free of information security incidents, it is possible to make these companies more secure day by day.

This research work has some limitations, namely regarding the large scope of the SMEs universe and the various disparities between a micro and a big enterprise.

Therefore, among future works which can be conducted, we highlight the definition of inhibiting factors to the implementation of an ISS policy in SMEs and the creation of a model of an information systems security policy which may be adopted and adapted by various companies according to their organizational culture.

References

1. ISO/IEC 27002. Information technology — Security techniques — Information security management systems — Requirements, International Organization for Standardization/ International Electrotechnical Commission (2005)
2. Beatson, J.G.: Information Security: The Impact of End User Computing. In: Gable, G.G., Caelli, W.J. (eds.) IT Security: The Need for International Cooperation — Proceedings of the IFIP TC11 Eighth International Conference on Information Security, pp. 35–45. Elsevier (1992)
3. Beal, A.: Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações, São. Atlas, Paulo (2005)
4. de Sá-Soares, F.: A Theory of Action Interpretation of Information Systems Security. PhD Thesis, University of Minho, Guimarães (2005)
5. Dhillon, G., Backhouse, J.: Information System Security Management in the New Millennium. Communications of ACM 43(7), 125–128 (2000)

6. ISO/IEC 17799. International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management, International Organization for Standardization/ International Electrotechnical Commission (2005)
7. Wood, C.C.: Writing InfoSec Policies. Computers & Security 14(8), 667–674 (1995)
8. Gaunt, N.: Installing an appropriate information security policy. International Journal of Medical Informatics 49(1), 131–134 (1998)
9. Karyda, M., Kiountouzis, E., Kokolakis, S.: Information systems security policies: a contextual perspective. Computers & Security 24(3), 246–260 (2005)
10. Lopes, I.: The adoption of information security systems in the local public administration in Portugal, PhD Thesis, University of Minho, Guimarães (2012)
11. Siponen, M.: A conceptual foundation for organizational information security awareness. Information Management and Computer Security 8(1), 31–41 (2000a)