Definition of Information Systems Security Policies

Isabel Maria Lopes[1,2,3(✉)], João Paulo Pereira[2,3], and Pedro Oliveira[3]

[1] Centro ALGORITMI, Universidade do Minho, Braga, Portugal
isalopes@ipb.pt

[2] UNIAG (Applied Management Research Unit), Instituto Politécnico de Bragança,
Bragança, Portugal
jprp@ipb.pt

[3] School of Technology and Management, Polytechnic Institute of Bragança, Bragança, Portugal
pedrooli@ipb.pt

Abstract. Information systems security (ISS) is crucial in all and each one of the services provided by organizations. Among security measures, policies assume a central role in literature. A lot has been said about this issue over the last years, however, the analysis of some studies conducted by different authors show that this ISS measure has not yet been institutionalized in most companies. By approaching aspects intrinsically related to ISS policies, this paper aims to contribute suggestions of some actions which might be taken to formulate and implement an ISS policy. Methodologically, the study involved interviewing the officials in charge of information systems in 21 Small and Medium Sized Enterprises (SMEs) in Portugal. The results are discussed in the light of literature and future works are identified with the aim of enabling the implementation of ISS.

Keywords: Information security · Definition of security policies · Information systems security policies

1 Introduction

Information is considered to be the most critical asset in the business world and the management of the risks associated with information must become a pattern practice within the companies [1]. Therefore, the adoption of an Information Systems Security (ISS) policy for the protection of such an asset makes total sense.

Organizations handle increasingly larger amounts of information in technological supports, which makes continuously stricter and broader security controls indispensable. The technological process may work as a catalyst for threats but is not alone enough to ensure the effective security of information.

Just as if not more important than reaching the appropriate levels of information security within each organization is being able to maintain them. Having software and hardware which contributes to the security of information is not enough. Organizations must also have a security policy and a good security management so as to firmly anchor the efforts to protect the assets of the information system [2].

In order to better understand the concept of ISS policy, it is convenient to distinguish it from concepts such as norms, directives and procedures. Table 1 shows the differences between these concepts.

Á. Rocha et al. (eds.), *Recent Advances in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 571, DOI 10.1007/978-3-319-56541-5_23

Table 1. Concepts of policy, norm, directive and procedure.

Policies – Documents which guide or regulate the actions of people or systems within the ISS domain [3].
Norms – Documents which specifically refer to the implementation technologies, methods and procedures as well as other details, with an applicability timeframe inferior to that of policies due to their higher technical nature [4].
Directives – Descriptions of specific activities and tasks.
Procedures – Descriptions of "who" executes the specific tasks as well as of "how" to execute them.

The ISS policy is a document which must contain the security recommendations, rules, responsibilities and practices to be adopted by the company so as to reach a desirable pattern of protection of the information systems. Since the security policy has to be formulated according to the company where it is going to be implemented, its drafting is a complex task which complies with a series of features and components. Regardless of the amount of literature available about this issue, the formulation of the policy represents a difficult task for the company. Therefore, its definition reveals to be paramount.

This context represents the framework of this work, in which, after this introduction, we proceed to the review of literature regarding the value and protection of information. Consecutively in Sect. 3, we focus on the risk analysis and in Sect. 4, we approach the research strategy. Finally, we present the conclusions in the light of the results obtained from the research, we identify the limitations of this study and propose future works.

2 The Value and Protection of Information

Information represents an asset which as any other important asset to business, has a value to the organization and consequently needs to be appropriately protected. Nowadays, information may be seen as a base product similar to electricity, without which many companies cannot operate [5].

The use of information pervades all aspects of the business. Most organizations need their information systems to survive and prosper. Therefore, they must act seriously to protect information [6].

As a concept, information security was developed as much in width as in depth and since it became a responsibility of the company itself, it needs the involvement of a strong management system that may determine the way to achieve the goals efficiently and coherently [7]. Information security is defined by the norm [2] as the set of procedures aiming the protection of information against several types of threats so as to ensure the continuity of business, minimize the risks and maximize the investments return as well as business opportunities.

Understanding that information is priceless to a certain organization and that the reasons to protect it are plausible, the set of procedures mentioned above must be put into practice. This set of procedures consists of nothing more than the formulation and implementation of an ISS policy in the organization.

Literature suggests a consensus as far as the importance of an ISS policy is concerned, and it is viewed by several authors as the foundation of the security effort. This observation can be confirmed by the following statements:

> "… the security policy is the foundation sustaining the whole security" [8].
> "… it is the cornerstone of the efficiency of information security" [9].
> "… it is a crucial milestone to guide workers' behavior for the management and protection of information" [10].

Since information has currently become an essential factor for starting and maintaining a business, it needs to be protected. An efficient ISS policy represents the main basis for information security within an organization.

Information security involves technology, processes and people. The technical measures such as passwords, biometric data or firewalls are not alone sufficient to mitigate the threats to information. A combination of measures is needed in order to secure and protect information systems against potential risks or threats [11].

3 Risk Analysis

It is almost impossible to approach the issue of information security without coming across the term "Risk Analysis" or "Risk Management". Both terms are tightly related to the process of information security management, namely when it comes to organizations and institutions. They represent determining factors to the choice of security measures and controls to be implemented, varying according to the needs and goals of each organization regarding the maintenance of its information confidentiality, integrity and availability.

Similarly to what happens with information security and risk analysis, it is difficult to talk about risk analysis without bumping into some concepts related to this issue:

Vulnerability – Term usually used to define the fragility of an asset which can be explored by one or more threats [12]

Threat – A circumstance or event whose observation or occurrence translates into a set of negative impacts on a system or resource presenting one or more vulnerabilities likely to be explored by the given threat.

Impact – This concept concerns the result caused by the occurrence of a certain security event on one or more resources which normally results in direct or indirect harmful consequences to the given resources.

Risk – Potential associated with the exploration of one or more vulnerabilities of a resource (or a set of resources) by one or more threats, with a negative impact on the affected resources and consequently on the activity and business of the organization.

Risk Analysis is the name given to the process of collecting and identifying critical resources, determining the existing vulnerabilities and threats as well as their impact and probability of occurrence, and the subsequent calculation of the level of risk associated with each one of the resources.

As observed in Fig. 1, the risk analysis is conducted bearing in mind the exploration of a certain vulnerability by a threat (there is the intention, opportunity and capacity to be a threat) which may cause a more or less negative impact on the organization and can consequently be more or less harmful.

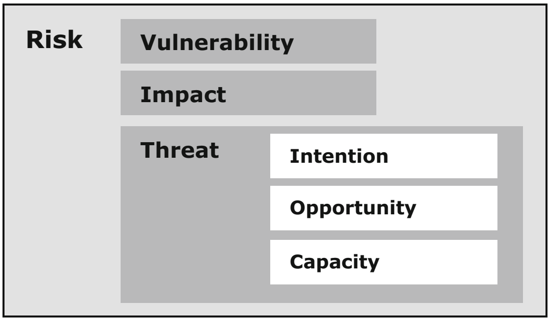

Fig. 1. Risk analysis

The risk analysis must be part of a permanent process of information security risk management capable of identifying new vulnerabilities and threats.

Such a risk analysis of the information system security is carried out in four stages [13]:

1. Risks identification – The identification of risks is achieved by acknowledging the risk context surrounding the organization. Several models can be used for this contextualization, among which we highlight the SWOT analysis (strengths, weaknesses, opportunities and threats). After this contextualization starts the identification of the elements necessary to the risk analysis: the threats, the vulnerabilities and the goods which might be in danger.
2. Risk and impact analysis – After identifying the threats, the next stage consists of characterizing risks by quantifying or qualifying the probability that those threats have of causing damage. An analysis of the impact on business must also be conducted by analyzing the critical activities for the survival of the company in case of disaster. This analysis may also be used for the creation of a business continuity plan against disasters.
3. Controls identification – The next step following the risk and impact analysis should be the identification and selection of the mechanisms allowing the reduction of the effect of the threat or damage. This identification of controls necessarily requires the definition of a structure for the information system security which must be based on a global strategy, so that the different interventions may be consistent with a global strategy, thus contributing to a higher maturity of the information system security.
4. Controls analysis – After identifying the controls, it is necessary to analyze them. The selection of the measure which will be applied results from this analysis and from the consequent reference of risk and impact. Among the several applicable measures, ISS policies are often used to protect the organizations' information systems from possible risks which may hinder their action.

One of the main priorities of the company in managing information is risk minimization, for which the organization must have a written information security policy [12]. Such a policy provides the formal guideline and intention of management regarding the protection of information in the company. It represents the structure for the definition of goals and norms to be implemented in order to mitigate risks to information [14].

4 Research Strategy

A field study was carried out through face-to-face semi-structured interviews with the officials in charge of the information systems in the Small and Medium Sized Enterprises (SMEs).

Considering the fact that this work addresses SMEs, it is essential to define this latter concept. The status of SME 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.

In Table 2, we present the number of workers and their representativeness within Portuguese business.

Table 2. Number of workers and percentage in 2012 in Portugal.

Type of enterprise	No. 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 table above, SMEs in Portugal represent 99.8% of business. Their representativeness is extremely high, which makes them deserve more attention in many respects.

In total, 21 SMEs workers were interviewed, evenly distributed among the three types, that is 7 Micro, 7 Small and 7 Medium sized companies.

As far as the process is concerned, the field study was developed through the following steps:

1. Elaborating the interview guides.
2. Elaborating the codebook.
3. Elaborating coding instructions.
4. Doing the interviews.
5. Transcribing the interviews.
6. Codifying the interviews.
7. Analyzing results.

These seven steps enabled us to carry out point 5 of this research work, in which we analyze a set of critical success factors to the implementation of an ISS policy in SMEs.

We also present a synthesis of the critical success factors to be borne in mind in each stage of the adoption process so that the whole procedure can be better understood.

5 Critical Success Factors

The development of an ISS policy is a critical activity. The credibility of the whole information security program of the organization depends on a well-drafted security policy [15].

The stages of the application process of an ISS policy in an organization (Formulation, Implementation and Adoption) are crucial to the correct adoption of a policy. However, other factors deserve all our attention as they are considered critical to the success of the ISS policy implementation.

The formulation of the policy is an indispensable element when managing information security within a company.

The policy document does not need to be very detailed, but it neither is a declaration of interests. The most important for it to be effective is to increase the awareness, understanding and commitment of all the parts involved.

The success of a policy strongly depends on its users' adoption and compliance. It is important to establish individual responsibilities for example, by clarifying who has access to a certain part of the system. For that, people must know, assume and comply with the security policy, norms and procedures in force, thus being committed to observing professional secrecy and the confidentiality of the data used in their work. They must also be committed to communicating possible security occurrences or problems they might detect with urgency and according to the established procedures.

Another aspect which is considered as a critical success factor to the good implementation is the definition of penalties for users who do not comply with the policy.

The support of the organizations' managers in the elaboration and implementation of the policies is also a critical factor essential to the success of an ISS policy. Only the involvement of all collaborators and especially the involvement of managers and heads of department will enable the achievement of a good elaboration and implementation of the policy.

ISS policies are often considered as a "live document" as they are never completed. Policies must be reviewed and if needed, updated periodically.

A policy will be of little use if it is not updated. Organizations are increasingly more dynamic and consequently, changes in structure and operating procedures occur at a fast pace. Therefore, it is necessary to adapt the policy to those new realities.

The timespan used for the review of a security policy varies from company to company. However, one thing is known, the review must be conducted whenever new facts are identified which are not accounted for in the existing version of the policy and may have an impact on security.

The policy communication and dissemination among all those who must acknowledge and observe it have also been considered paramount for the success of policies. We can easily accept that all users must know about the security policy. Although the ways to disseminate it may vary (internal memorandum, providing the policy in the organization's Intranet or other mechanisms), it is necessary to ensure that all have been informed of the content of the policy.

It is claimed that the security process starts immediately at the stage of recruitment. Organizations should attach the ISS policy to their workers or collaborators' working contracts.

Integrating policies along with the organization's goals, processes and culture is paramount to the success of the policy implementation. ISS policies must be a constructive and protective vehicle and never a mechanism which might hinder the development of the organization's activity. For that, before formulating a policy, the goals of the company as well as its organizational processes and culture must be taken into account.

The feasibility of the policies (as far as implementation and compliance are concerned) represents another essential factor. An ISS policy will be of little or no use if its feasibility reveals to be impossible.

It is necessary to raise the awareness of the people involved towards the fact that technology is not the only element to consider. Without an ISS policy or without mechanisms of response to occurrences or business continuity plans, technologies will not be effective in the protection of information within the organization.

Another aspect to bear in mind respects the awareness of users and leaders regarding security issues. Since the human factor is pointed out as the responsible one for most security occurrences, peoples' awareness is crucial so as to allow the organizational ISS policy to produce the desired result.

As expected in all processes involving change, there is a natural resistance from people. In the particular case of information security, there is another detail which is the "misinformation on the issue". People do not easily understand, at least not initially, the real motive and need for so many controls, processes and evidences. It is not rare to see some quite varied reactions when implementing some action targeting the promotion of security.

The support of the organization board is paramount for the information security policy to be effective, thus starting any action in this direction without such support is foolhardy, to say the least.

The executive board or the people in charge of the organization must be responsible for promoting and supporting the establishment of security measures which may ensure the integrity, availability and confidentiality of their computer assets with the purpose of avoiding their possible alteration, destruction, theft, copy, forgery or any other existing threats, whether unintentional or not.

There is consensus in literature regarding the fact that the biggest threat to information security lies on careless workers who do not comply with what is established in the organizations' information security policies and procedures. Therefore, workers must not only be aware of the content of the policies but must also comply with the organization's information security policies and procedures [16].

The security policy must only be put into practice after users have been informed of its content, after they have been trained and after they have signed a declaration of commitment.

Furthermore, the provision of regular training on information security to collaborators is not only essential but it is what will actually ensure a successful application of the guidelines contained in the information security policy.

An effective and somewhat easy way to raise workers' awareness towards information security issues is to provide policies which are understandable to all the workers of the organization and which are easily available at any given time [17].

We consider these aspects to be critical success factors to the institutionalization of a security policy. For a clearer display, Tables 3, 4 and 5 present a synthesis of the critical success factors to be taken into account in each stage of the policy adoption process, according to the 21 interviews conducted in the SMEs.

Table 3. Critical success factors during formulation.

Formulation
- Risk assessment
- Defining goals for security
- Existence of political willingness
- The document must be well-drafted
- The document must not be long
- Approval of the executive board

Table 4. Critical success factors during implementation.

Implementation
- Defining the way for the document to reach users
- All users must be familiar with the document
- Explaining to users the advantages of having a policy
- Establishing responsibilities for both users and those in charge of implementing the policy
- Defining penalties
- Engagement and commitment in the implementation

Table 5. Critical success factors during adoption.

Adoption
- Monitoring compliance with the policy
- Capacity to penalize users
- Investing in users' training
- Reviewing the policy periodically
- Updating the policy
- Solving possible conflicts and difficulties in applying the security parameters

Above all, it is important to highlight that the new reality we live in as far as new information and communication technology is concerned demands higher levels of attention regarding ISS. The use of information pervades all aspects of a business as well as of our lives. Most organizations need an information system in order to survive and thrive. Therefore, they need to be very strict in the protection of their information assets.

The institutionalization of ISS policies must become a reality within organizations, regardless of their size or of their area of business. However, due to their high number, SMEs deserve even more attention.

6 Conclusions

This study identified a set of factors which condition the adoption of ISS policies in Portuguese SMEs. Besides this contribution, this paper brought forward guidelines which are believed to enhance the institutionalization of ISS policies in SMEs in Portugal.

The ISS policy must be the guideline to be followed by a company in order to keep their most valuable information safe, whether it is essential information for the daily decision-making of the company or previously filed information.

Keeping in mind the activity of the company and whatever is required by such activity, it is convenient to formulate a policy that is clear and concise, without any rules which might not be obeyed when the policy is implemented due to the specific characteristics of the company.

Besides the implementation of an ISS policy, we also recommend its monitoring. Having an excellent security policy is not enough if it is not being adopted by the users of the system. The same happens to updating, since no matter how good the ISS policy is, it will never be an asset for the company's information security if it is not updated.

One of the limitations of this research work is related to the circumscription of the study to 21 SMEs. Although we believe that enough data was collected for the purpose of this work, we understand that a study conducted in more companies could result in a richer and more grounded set of data.

Among future works which might be undertaken, we highlight a recommendation in the form of a proposal containing the elements that an ISS policy might comprise. The aim of such a work would be to try to invert the incipient numbers of policies currently existent in companies by using the proposal as a potential model to follow.

Acknowledgments. UNIAG, R&D unit funded by the FCT – Portuguese Foundation for the Development of Science and Technology, Ministry of Science, Technology and Higher Education, Project no. UID/GES/4752/2016.

References

1. Broderick, J.S.: Information security management – when should it be managed? Inf. Secur. Tech. Rep. 3, 12–16 (2001)
2. ISO/IEC 17799: International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management, International Organization for Standardization/International Electrotechnical Commission (2012)
3. de Sá-Soares, F.: A theory of action interpretation of information systems security. Ph.D. thesis, University of Minho, Guimarães (2005)
4. Wood, L.: Writing InfoSec policies. Compute. Secur. **14**(8), 667–674 (1995)
5. Carr, N.G.: It doesn't matter. Harvard Bus. Rev. 41–9 (2003)
6. Van Niekerk, J.F., Von Solms, R.: Information security culture: a management perspective. Comput. Secur. **29**, 476–486 (2010)
7. Ashenden, D.: Information security management: a human challenge? Inf. Secur. Tech. Rep. **13**, 195–201 (2008)
8. Shorten, B.: Information security policies from the ground up. In: Tipton, H.F., Krause, E.M. (Eds.) Information Security Management Handbook, 5th edn. Auerbach, Boca Raton, pp. 917–924 (2004)
9. Cardoso F. Oliveira, P.: Política de segurança da informação nas empresas, Faculdade de Tecnologia de Ourinhos - FATEC (2013)
10. Da Veiga, A.: The influence of information security policies on information security culture: illustrated through a case study. In: Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), pp. 22–33 (2015)
11. Da Veiga, A., Eloff, J.H.P.: An information security governance framework. Inf. Syst. Manag. **24**(4), 361–372 (2007)
12. ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management (2013)
13. Silva, P.T., Carvalho, H., Torres, C.B.: Segurança dos Sistemas de Informação – Gestão estratégica da segurança empresarial, Centro Atlântico (2003)
14. PricewaterhouseCoopers: The Global State of Information Security Survey, http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml
15. Kadam, A.W.: Information security policy development and implementation. Inf. Syst. Secur. **16**(5), 246–256 (2007)
16. Siponen, M., Pahnila, S., Mahmood, A.: Employees' Adherence to Information Security Policies: An Empirical Study. In: Venter, H., Eloff, M., Labuschagne, L., Eloff, J., Solms, R. (eds.) SEC 2007. IFIP, vol. 232, pp. 133–144. Springer, Boston, MA (2007). doi: 10.1007/978-0-387-72367-9_12
17. Haeussing, F., Kranz, J.: Understanding of information security awareness – an emperical study. In: Proceedings of the 19th Americas Conference on Information Systems (2013)