Advances in Intelligent Systems and Computing 444

Álvaro Rocha
Ana Maria Correia
Hojjat Adeli
Luis Paulo Reis
Marcelo Mendonça Teixeira *Editors*

New Advances in Information Systems and Technologies

Volume 1

Springer

Architecture of Information Security Policies: A Content Analysis

Isabel Lopes[1] and Pedro Oliveira[2]

[1]Centro ALGORITMI, Universidade do Minho
[1 2]School of Technology and Management, Polytechnic Institute of Bragança, Portugal
{ isalopes, pedrooli }@ipb.pt

Abstract. The growing importance that Information Systems (IS) have in our companies naturally brings about a need to rely and trust in their use. There are a number of technologies which help ensure the security and trust in the IS use. However, technology alone does not solve all the problems, which is why there is a need for well-defined information systems security policies in order to ensure the data integrity and confidentiality. Nevertheless, there is a lack of information concerning the contents that such policies must have. This work aims to contribute to the filling of this gap. It presents a synthesis of the literature on information security policies content and it characterizes 15 Small and Medium Sized Enterprises (SMEs) information security policy documents as far as their features and components are concerned. The content analysis (CA) research technique was applied to characterize the information security policies. The profile of the policies is presented and discussed and propositions are made for possible future works.

Keywords: Features and Components of Information Security Policies, Information Security, 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. Among information security controls, the literature gives a central role to information security policies.

Despite the significant number of studies on the topic of information systems security (ISS) policies, until mid-2000s the literature revealed a limited number of

Á. Rocha et al. (eds.), *New Advances in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 444,
DOI 10.1007/978-3-319-31232-3_46

empirical studies on this security measure. Indeed, some authors had pointed to limitations on the research performed, such as the inexistence of a coherent theory about information security policies [4] and the inexistence or low expression of empirical studies focusing on the adoption, content and implementation of information security policies [5,6]. Since the time when these observations were made, several studies of empirical nature on ISS policies have arisen, such as [7]. The majority of the works in this last set of studies promoted surveys that addressed the intentions and behaviors of employees, examining factors which facilitate or inhibit compliance with ISS policies. These works, however, did not consider the specific ISS policy documents held by organizations nor the connection between the wording in those documents and employees' behaviors or intentions to protect information systems assets.

The literature on this topic may have been enrichened, but its focus can be quite wide. As it is not viable or even conceivable to address all the aspects regarding ISS policies, we decided to focus this work on their content. Therefore, we studied 15 ISS policy documents formally adopted in SMEs and centered our analysis on their content.

The paper is structured as follows. After this introduction, we review the literature on the features and components of information security policies. Then, the research questions are presented and the research strategy is described. Afterwards, we present the main results of the study. The paper ends by drawing conclusions and suggesting future work.

2 Architecture of Information Security Policies

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 [8].

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. For [9], 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.

The ISS policy is a document which must describe the recommendations, rules, responsibilities and security practices to be adopted by the company so as to achieve a desirable standard of information systems protection. Since the security policy has to be formulated according to the company in which it is going to be implemented, its drafting is a complex task and complies with a series of features and components. These two points constitute the content of an ISS policy and are therefore defined below.

2.1 Features of Information Security Policies

One of the policies main features is the way they are structured, with different authors recognizing different forms of structuring. The author [10] acknowledges the existence of organizational policies, which establish general guidelines for the information security program, and of technical policies, which establish the security requirements that a product or a computer system should observe. In turn, [11] acknowledge the existence of three fundamental structures for policies:

- Individual policy – In this structure, the organization creates a separate and independent security policy for each technology and system used.
- Complete policy – In this structure, which is the most common according to the authors, the organization centrally defines, controls and manages one single document which includes all the technologies used and provides general guidelines to all the systems used by the organization.
- Modular complete policy – This policy is centrally controlled and managed as in the case of the complete policy, and it consists of general sections, with descriptions of the technologies used, and discussions about the systems responsible and appropriate use. For this author, this is the most effective structure for information security policies.

An additional important feature is related to the policies language. Security policies must be written in a simple and understandable language, free from technicalities and ambiguous terms which may prevent their clear understanding. Their precision must not be jeopardized, which is why a policy must be written in a clear way, thus not generating any doubt or question from its recipients.

The length of a policy depends on the amount and complexity of the systems and agents that it covers, as well as the level of abstraction applied in its writing, since a document with a high level of abstraction will not come into extensive detail. The author [12] recommends a length ranging between one and five pages.

The most common approach is a policy containing few words and that is widely directed. Therefore, its text must be direct, succinct and concise.

The way the policy will be disseminated among all the users of the information system must also be taken into account. The policy may be provided in paper or in digital format. This aspect must be analyzed according to the kind of company so as to ensure that the dissemination is as effective as possible.

Finally, but not less important, security policies must follow a periodic updating process subject to relevant organizational changes such as: staff increase, changes in the computerized infrastructure, high staff rotation, development of new services, regionalization of the company, change or diversification of the line of business, etc. The periodicity of the policy review ranges from six months to one year.

2.2 Components of Information Security Policies

Although it is accepted that an ISS policy may vary considerably from organization to organization, this possibility has not prevented some authors from bringing forward some guidance on the elements that policies should typically include.

By comparing several information security standards, Hone and Eloff isolated the following elements as generic components that ISS policy should include [12]:

- Need for and Scope of Information Security
- Objectives of Information Security
- Definition of Information Security
- Management Commitment to Information Security
- Approval of the Information Security Policy
- Purpose or Objective of the Information Security Policy
- Information Security Principles (risk management, compliance, access control, etc.)
- Roles and Responsibilities
- Information Security Policy Violations and Disciplinary Actions
- Monitoring and Review
- User Declaration and Acknowledgement
- Cross References (to other information security documents)
- General Elements (authors, date of policy and review date of policy)

Defining a security policy which:

- Includes the organization's information security general framework and goals
- Considers legal or contractual requirements regarding information security
- Is aligned with the risk management strategic context of the organization in which the ISS policy is being implemented and maintained
- Establishes the criteria for evaluating risk
- Is approved by the direction.

Most certainly, one of the main points to be defined in an ISS policy is the goal and target of its corresponding information system, its priorities regarding services, users, methodologies and technologies, among others. Thus, one of the most important aspects to be considered is the scope of action that the policy intends to establish.

The following policy structure can be used as a basis for creating information security common policies [13]:

- Policy Title: Name of the Policy Area
- Policy Purpose: Briefly illustrates the purpose of the Policy
- Policy Applicability: Defines various internal and external entities as well as the people to which a particular Policy statement will apply
- Executive Owner: Identifies the person who has the ultimate authority and responsibility for any changes and updates in the policy. Any changes or updates in the policy have to be approved by the Executive Owner
- Custodian: The person who is responsible for maintaining, communicating, and updating the policy based on directions from the Executive Owner
- Enforcement: Defines the consequences of any violation of the policy
- Policy Sub Area: Defines sub areas of a policy area, e.g. Logical Access Management – Access Control
- Policy Statement: This section describes the control statements' part of the specific policy
- Policy Effective Date: This section defines the date from which the policy is applicable and is to be followed

3 Research Strategy

Since the aim of this work is to analyze the documents which go under the name of ISS policies, we started with a literature review, always focusing on the features and components of a policy. Subsequently, we had to collect ISS policies. Given the intention of making a comparison between several policy documents, we decided to restrict the collection of documents to a single group of enterprises. With this option, we sought to minimize the possibility of documents belonging to different enterprises having different features and components, due to particular characteristics of each of those enterprises as well as specific information security needs.

The enterprises that we selected for the collection of the policies was that of SMEs. These enterprises was chosen for two main reasons. Firstly because in Portugal, SMEs represent 99.8% of business. Their representativeness is extremely high, which makes them deserve more attention in many respects. Secondly, because when focusing our attention on SMEs, a study carried out by [14] revealed that among the 307 SMEs surveyed, only 15 stated to have an ISS policy. One of the conclusions drawn from that study was that the implementation and consequent adoption of an ISS policy has not yet become a reality in SMEs.

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 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

3.1 Research Questions

The analysis of the documents enables us to globally list the features and components of the 15 ISS policies under study. Among the features and components, there are some specific issues which deserve our attention.

Thus, with respect to the policies' features, we will address the following issues:

1. What is the length of the policy documents?
2. How are the policies written?
3. What is the expected durability of the policy documents?
4. What is the structure of the policies?
5. How are the policies delivered?
6. What kind of documents are the policies?

With respect to the policies' components, we put forward the following specific questions:

1. What components do the policies contain?
2. Are there any components that make part of all the policy documents?
3. Are there any components that are not present in any of the policy documents?
4. What is the purpose of the policies?
5. What is the scope of the policies?
6. What kinds of responsibilities do the policies determine?

3.2 Research Method

The use of a research method is paramount since it represents the means to an end. A research methodology does not look for solutions but chooses the way to find them, integrating knowledge through the methods which are applicable to the various scientific or philosophical subjects. Although there are several ways to classify them, research approaches are normally distinguished between quantitative and qualitative [15]. It is acknowledged that the choice of the method must be made according to the nature of the problem being addressed. Therefore, we considered appropriate to follow a quantitative research method (traditional scientific research), based on the positivist rational thought, according to which through empirical observations, we build theories (expressed in a deductive way) that try to explain what is observed. Among the possible research methods to use, we applied the CA.

CA is a method which differs from the other research methods because instead of interviewing or observing people, the researcher deals with pre-existing records and interferes based on those records.

CA is a research technique for the objective, systematic, and quantitative description of manifest content of communications. So that this description can be objective, it requires a precise definition of the analysis categories, in order to enable different researchers to use them and get the same results. So that it is systematic, the whole relevant content must be analyzed in relation to all the meaningful categories. Finally, quantification allows the provision of more precise and objective information concerning the occurrence frequency of content features [16].

4 Results

The aim of the study is to characterize the content of ISS policy documents that have been adopted by SMEs. Such characterization will be made by answering the twelve research questions listed in point 3.1.

The length of the documents analyzed ranges from a maximum of 10 pages and a minimum of one page. The average length is 3.6 pages. With regard to the number of words, the documents analyzed ranged between a maximum of 3987 words and a minimum of 212 words, with a mean of 1266 words.

Most ISS policies are easy to read and understand, appropriately structured and written in a clear and intelligible way. Some documents use a number of technical

terms from the information security domain, but there is a concern to define them either immediately after their use or grouped in a list containing the respective definitions.

None refers to the durability of the document or to the periodicity in which the policy must be revised.

Another finding from the analysis of the 15 documents is that none of them constitutes a purely technical ISS policy. The analyzed documents can be classified as organizational policies.

With respect to the way the policy is delivered to the users of the SME Information System so that they become acquainted with it, we found that in 9 of the cases (60%), the policy is handed in person by the head of the IT department. In the remaining cases, the policy is delivered in digital format.

Among the 15 policies, 14 (93%) have a clearly identifiable title. Nevertheless, the title of the documents varies considerably, though they may be grouped into the following categories: regulation (six cases), norm (five cases), manual of rules and procedures (one case), job instructions (one case), rule (one case) and policy (one case). Despite this variety, most of the titles include a reference to IS or IT, such as information, IT equipment, email, internet, computers, and applications.

In Table 2, we present the components of a policy as well as the frequency of their presence in the 15 documents.

Table 2. Components Contained in the Information Security Policies

	Policies																
Components	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**Nº**	**%**
Objective of the information security		X			X				X	X						4	27
Purpose of the policy		X	X	X	X		X	X	X		X	X		X	X	11	73
Scope of the policy		X	X				X	X		X	X	X	X	X	X	10	67
Definitions				X	X				X							3	20
Guidelines		X														1	7
Requirements	X	X	X	X	X	X		X	X	X	X	X			X	12	80
Directives		X	X	X	X	X	X	X	X	X	X	X	X	X	X	13	87
Responsibility	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	15	100
Responsibility of the owner		X									X					2	13
Communication of incidents										X					X	2	13
Allocation of resources		X						X	X							7	47
Punishments			X	X	X		X	X	X		X	X		X	X	10	67
Communication procedure			X												X	2	13
Policy communication targets		X	X	X										X		4	27
Statement of notification	X	X		X	X			X						X		6	40
Location of the policy							X	X						X	X	4	27
Author of the policy	X	X	X						X			X	X			6	40
Date of approval		X		X		X	X		X	X		X		X		8	53
Date of entry into force										X	X					2	13
Approval of the policy		X		X		X	X	X		X	X	X		X		9	60
Contacts	X		X	X	X		X	X	X	X	X	X	X		X	12	80

The components which are present in more than 50% of the documents are listed here in a decreasing order of frequency: Responsibility, Directives, Requirements, Contacts, Purpose of the policy, Scope of the policy, Punishments, Approval of the policy and Date of approval. Among these components, only one is universal to the 15 documents, namely responsibilities.

With regard to the components which are not present in any of the documents, we can highlight the following: Executive summary, Relation between security and business objectives, Coordination among organizational entities, Ethics concerning information security, Threats, Review date of policy and Approval of reviews.

In some documents, the purpose of the policy was stated as the reason for the formulation of the policy and in other documents to specify what the SME wants to achieve with the policy. The incidences of the purpose are the IT resources (nine cases), internet and email (one case), information (one case).

As far as responsibilities are concerned, the major types of responsibilities allocated to users or organizational units, i.e., those that appear in more than half of the documents, are listed in Table 3.

Table 3. Types of Responsibilities

	Policies																
Responsibilities	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**Nº**	**%**
Information security policy	X	X	X		X			X	X			X			X	8	53
Internal organization of information security			X						X						X	3	20
Responsibility for assets		X	X		X	X	X	X	X	X	X	X	X	X	X	13	
Secure areas								X	X						X	3	20
Operational system access control			X		X	X	X	X	X		X	X		X	X	10	67
Protection against malicious code	X	X			X			X	X		X	X		X	X	9	60
Backup			X		X	X	X	X	X		X	X		X	X	10	67
Security management network		X	X	X	X			X	X	X		X	X			9	60
Media Handling		X					X							X	X	4	27
Exchange of information	X	X										X		X		4	27
Monitoring							X						X	X	X	4	27
Requirements for access control			X					X							X	3	20
User access management								X							X	2	13
User responsibilities		X	X		X			X	X			X			X	7	47
Network access control		X			X		X	X	X		X			X		7	47
Operating system access control					X		X	X	X		X			X	X	7	47
Application and information access			X					X	X						X	4	27
Of the IS safety requirements							X								X	2	13
Security of system files					X	X	X	X	X			X	X	X	X	9	60
Security in development and support processes		X			X		X		X		X		X	X	X	8	53
Compliance with legal requirements								X	X					X	X	4	27
Compliance with the security norms							X	X	X						X	4	27
Other information security object					X		X				X					3	20

The responsibilities which appear in over 50% of the documents are listed here in a decreasing order of frequency: Responsibility for assets, Operational systems access control, Backup, Security management network, Protection against malicious code, Security of systems files, Security in development and support processes, Information security policy.

With respect to the responsibilities which are not contained in any of the analyzed documents, we can highlight the following: Information Classification, Security Equipment, Cryptographic Controls, Job Changing, Before Employment.

5 Conclusions

This study involved the analysis of 15 ISS policies adopted by SMEs and focused on the features and components of the policies. This work contributes to the literature by analyzing information security empirical materials and bringing more practical and practitioner oriented perspectives to information security research. By focusing on the substance and form of actual ISS policies, it elucidates an area of information security research that has been largely ignored, in spite of its practical relevance for the improvement of information security by organizations and it supplements the literature whose traditional focus has been on individual intentions towards ISS policies.

Within this context, we consider that, in order to achieve organizations' wellness, it is important to implement security measures which take into account the confidentiality, integrity and availability of the information contained in information systems [17,18] so as to prevent, detect and respond to the threats which such systems are exposed to and therefore, protect information.

The research method used in the analysis of the documents was the content analysis. Since it consists of a technique aiming at an objective, systematic and quantitative description of the symbolic behavior and since its object is the content of communication, the content analysis revealed to be the appropriate method for this kind of research.

This research work has some limitations, namely as far as the number of documents collected and the delimitation of the study to SMEs are concerned. We must point out that a more significant number of documents would lead to a more sustained analysis. However, it is important to acknowledge that the adoption of ISS policies is not institutionalized in SMEs, and also that these policies are usually documents strictly reserved for the company, which makes it difficult to access this type of security control.

In the light of all this, among future works which can be conducted, we highlight 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. Another possible work may consist of relating the content of the policies which were analyzed to the recommendations found in literature.

Acknowledgment

This work has been supported by FCT - Fundação para a Ciência e Tecnologia within the Project Scope UID/CEC/00319/2013

References

1. ISO/IEC 27002: Information technology — Security techniques — Information security management systems — Requirements (2005)
2. Beatson, J. G.: Information Security: The Impact of End User Computing. In G. G. Gable e W. J. Caelli (Eds.), IT Security: The Need for International Cooperation — Proceedings of the IFIP TC11 Eighth International Conference on Information Security, Amsterdam, 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 Paulo: Atlas (2005)
4. Hong, K.S., Chi, Y.P., Chao L.R., Tang J.H.: An integrated system theory of information security management. Information Management & Computer Security, 11 (5), 243-248 (2003)
5. Fulford, H., Doherty, N.F.: The application of information security policies in large UK-based organizations: an exploratory investigation. Information Management & Computer Security, 11 (3), 106-114 (2003)
6. Knapp, K., Marshall, R., Rainer, K, Ford, N.: Information Security: Management's Effect on Culture and Policy. Information Management & Computer Security, 11 (1), 24-36 (2006)
7. Karyda, M., Kiountouzis, E., Kokolakis, S.: Information systems security policies: a contextual perspective. Computers & Security, 24 (3), 246-260 (2005)
8. ISO/IEC 17799 International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management, International Organization for Standardization/International Electrotechnical Commission (2005)
9. Wood, C. C.: Writing InfoSec Policies, Computers & Security, 14 (8), 667-674 (1995)
10. Lindup, K.R.: A New Model for Information Security Policies. Computers & Security, 14 (8), 691-695 (1995)
11. Whitman, M.E., Townsend, A.M., Aalberts, R.J.: Information Systems Security and the Need for Policy, In Information Security Management: Global Challenges in the New Millennium (Dhillon, G. Ed.), Idea Group Publishing (2001)
12. Höne, K., Eloff, J.: Information security policy – what do internationalinformation security standards say? Computers & Security, 21 (5), 402-409 (2002)
13. Communications and Information Tecnology Commission, Information Security Policies and Procesures Development Framework for Government Agencies http://www.citc.gov.sa/English/RulesandSystems/RegulatoryDocuments/OtherRegulatoryDocuments/Documents/CITC_Information_Security_Policies_and_Procedures_Guide_En.pdf
14. Lopes, I., Oliveira, P.: Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises. Álvaro Rocha et al (eds.). New Perspectives in Information Systems and Technologies, Volume 1. ed. Cham: Springer International Publishing, v. 275, p. 277-286 (2014)
15. Myers, M. D.: Qualitative Research in Information Systems ACM Computing Surveys (CSUR), MISQ Discovery (1997)
16. Berelson, B.: Content Analysis in Communications Research. Free Press, New York (1952)
17. Kim, D., Solomon, M. G.: Fundamentals of Information Systems Security, Jones and Bartlett Publishers (2010)
18. Tipton, H., Krause, M.: Information Security Mangement Handbook. Auerbach Publications (2009)