INFORMATION SYSTEMS SECURITY POLICIES: A SURVEY IN PORTUGUESE PUBLIC ADMINISTRATION

Isabel Maria Lopes
Instituto Politécnico de Bragança, Portugal

Filipe de Sá-Soares
Universidade do Minho, Portugal

ABSTRACT

Information Systems Security is a relevant factor for present organizations. Among the security measures, policies assume a central role in literature. However, there is a reduced number of empirical studies about the adoption of information systems security policies. This paper contributes to mitigate this flaw by presenting the results of a survey in the adoption of Information System Security Policies in Local Public Administration in Portugal. The results are discussed in light of literature and future works are identified with the aim of enabling the adoption of security policies in Public Administration.

KEYWORDS

Information System Security Policies, Information System Security in Public Administration, Information System Security.

1. INTRODUCTION

Information Systems Security (ISS) is a crucial issue for most organizations. With the advent of information technology (IT) and the massive use of the Internet and its services, the number of attacks to which information is subject is increasingly higher and, consequently, the need to protect information systems (IS) is becoming imperious.

Security policies have a central role in ISS literature, appearing as one of the crucial factors to the information security of an organization.

There are a reasonable number of studies focusing on security policies in the ISS research domain. However, this number is significantly reduced when we consider empirical works on the adoption of security policies. This reality has been highlighted by several authors, who have pointed out certain limitations to the research done on that area. The main criticisms are related to the inexistence of a coherent theory about security policies [Hong et al. 2003], inexistence or low expression of empirical studies focusing on the adoption, content and implementation of ISS policies [Fulford and Doherty 2003; Knapp et al. 2006], lack of empirically supported research on ISS [Kotulic and Clark 2004] and a concern which is too centered in policies content and structure, and in the problem of gathering management support with respect to policy formulation, implementation and enforcement [Baskerville and Siponen 2002].

This fact brings about a difficult issue, as it raises the question about the real agreement between what is claimed in literature about ISS policies and what is actually done in practice.

Although each organization has specific needs in terms of ISS, Public Administration constitutes an interesting sector to conduct research on IS, as suggested by the fact of being one of the major investors in IT [Gartner 2009] and due to the specific challenges it raises [Bretschneider 1990, Newcomer and Caudle 1991]. Among the various Public Administration institutional agents, the City Councils assume a specific relevance, as they condense a growing strong demand from their citizens for information services, and for the information diversity and quantity they deal with in the performance of their duties. Therefore, the efficiency of their IS is crucial. Due to the information they receive, store, process and distribute, the security of their IS is indispensable to their normal functioning and to the protection of personal data which they are trusted with.

In the case of Local Public Administration in Portugal, the studies focusing on ISS are almost inexistent. Indeed, we only found two governmental technical reports (cf. [OSIC and UMIC 2004, 2006]), whose primarily concern was on the use of IT by Portuguese municipalities, that included some data regarding ISS, although limited to security technologies employed and to the main security problems faced by municipalities. Consequently, the first difficulty we come across is a general lack of knowledge about the Portuguese City Councils reality concerning the adoption and application of ISS policies.

Bearing in mind this difficulty, we have tried to mitigate the gap identified in literature by conducting a survey directly in the 308 Portuguese municipal entities. The survey consisted of a number of questions about ISS policies, focusing on the existence and features of such documents.

This is the context of the present work, which aims to find out about the Portuguese City Councils reality as far as their ISS is concerned, as well as to quantify those which have adopted ISS policies.

The structure of the paper is as follows. After this introduction, we briefly review the literature on ISS policies in terms of policies' importance, features and components. Then, in Section 3, we state the research purpose that motivated the promotion of a survey to characterize the adoption of ISS policies by Portuguese City Councils. On Section 4, the survey, its target population, structure and results are presented. In the subsequent section the findings are discussed. In the last section, taking into account the results of the study we identify future work opportunities.

2. INFORMATION SYSTEMS SECURITY POLICIES

Information is one of the present organizations main assets. Therefore, it is natural that the systems supporting information are increasingly exposed to either intentional or accidental threats. These threats put at risk the confidentiality, integrity and availability of information and systems which manipulate it. Consequently, the people in charge of organizations should consider and implement measures aiming to prevent, detect and respond to such threats.

In order to succeed in their IS protection actions, organizations need to adopt several types of measures. They need to implement not only ISS technical measures, but also and increasingly more organizational and social measures, as this is the only way to reach organizational well-being as well as maintain organizations integrity [Dhillon and Backhouse 2000].

ISS policies have been pointed out in literature as the most appropriate and indispensable way to launch and sustain the organizations' ISS program, so that organizations may achieve a certain security level of their IS.

Considering the present technology and business context, organizations have to stop worrying only about *crackers* attacks or *firewalls* and antivirus implementation, to start focusing on the creation of a wider and more complete and complex ISS policy. As noticed by Wood [1995], only by setting up a firewall, we cannot ensure that, for example, the Internet access is safe. There is the need to consider several other issues, such as policies, procedures, standards and guidelines which will direct users' actions.

2.1 Importance

Literature review suggests a high level of agreement on the importance of an ISS policy in organizations, being considered by several authors as the foundation of the security effort. This recognition can be observed in the following statements:

> "The security policy is to the security environment like the law is to a legal system. (…) A policy is the start of security management." [Higgins 1999, p. 217]
>
> "... a digital system without a security policy is likely to have a hodge-podge of countermeasures. The policy is what ties everything together." [Schneier 2000, p. 308]
>
> "An effective information security policy is as necessary to a good information security program as a solid foundation is to a house." [King et al. 2001, p. 13]
>
> "The cornerstone of an effective information security architecture is a well-written policy statement." [Peltier 2002, p. 21]

> "The information security policy is one of the most important documents in an organization..." [Höne and Eloff 2002a, p. 409]
>
> "... the security policy is the foundation on which all security is based." [Shorten 2004, p. 917]
>
> "Security policies are the foundation and the bottom line of information security in an organization." [Kee 2001, p. 1]

The increasing high level of importance given to ISS policies can be explained by the use that these documents reveal to have in terms of the initiatives developed by organizations for IS protection [de Sá-Soares 2005].

According to Höne and Eloff [2002a], security policies are a privileged vehicle for the people in charge to explain the need for security in the organization information system.

Policies also reveal their usefulness through the establishment of the major ISS guidelines, giving direction to the information system protection initiatives, and defining the role that ISS plays in supporting the organizational mission and goals [JISC 2001].

ISS policies are also important for security personnel, since they provide indications about the assets the organization wants to protect and the protection degree which is to be given to each of those assets [King et al. 2001].

In addition to that, ISS policies assist in the coordination of IS protection actions, preventing the fragmentation of efforts and acting as a guide in the process of selection, development and implementation of ISS controls [Barman 2001].

Another aspect we can highlight is the ISS policy contribution to the organization as a whole, so that everyone behaves in a coherently acceptable way as far as information security is concerned [Lee 2001].

We can also refer its role in the assurance that the organization is complying with the appropriate legislation, namely by avoiding or limiting civil or criminal responsibilities [Dhillon and Backhouse 1997].

2.2 Features

In what concerns the features of a security policy, Höne and Eloff [2002b] claim that the policy document should not include the technical aspects related to the implementation of security mechanisms, as these may change throughout time. On the other hand, it should be a document which is easy to read and understand, short, and written with a high abstraction level in mind. Finally, with respect to its durability, policy reviews should be carried out on a regular but not constant basis.

Many of the factors listed above are shared by Kee [2001], who thinks the first thing to bear in mind when writing a policy is to write it in a language that is easy to understand instead of making it complicated. To this author, policies should be written using the SMART rule, which stands for ***S**pecific, **M**easurable, **A**greeable, **R**ealistic and **T**ime-bound*.

Another aspect to consider is related to the structuring of ISS policies statements. Different authors support different structuring ways.

Lindup [1995] acknowledges the existence of organizational policies, which establish general guidelines for the ISS program, and technical policies, which establish the security requirements that a computer product or system to be developed should observe.

In contrast, Baskerville and Siponen [2002] distinguish three ISS policies categories:

- **High level policies** – They consist of high level global plans which include the general goals and acceptable procedures in the realm of ISS.
- **Low level policies** – They are information security action methods, defined and selected among the various alternatives and in the light of certain data and conditions which guide and determine the present and future information security decisions.
- **Metapolicies** – They are the "policies for the policies", in other words, the organizational guidelines for the policies formulation and maintenance.

Apart from those, Whitman et al. [2001] observe three fundamental structures for ISS policies:

- **Individual policy** – In this structure, the organization creates a separate and independent security policy for each technology and system in use.

- **Complete policy** – According to 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 systems used by the organization.
- **Modular complete policy** – This policy is centrally controlled and managed as it is 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. It differs from the previous structure because it includes modular appendixes, which provide specific details on each technology and bring forward particular observations, differences, restrictions and functionalities related to the use of technology which are not properly covered in the base policy document. For these authors, this is the most effective structure for ISS policies.

2.3 Components

As far as components are concerned, some authors warn us about the dependence of these documents composition on the organization nature, size and goals, making difficult the generalization of elements which must be part of a security policy.

Although it is accepted that an ISS policy varies considerably from organization to organization, to Wood [1995] this document should typically include the following elements: general statements of aims, goals, beliefs and responsibilities, frequently accompanied by general procedures for their achievement.

Whitman [2004] defines that a good ISS policy should outline individual responsibilities, define which users are allowed to use the system, inform workers about potential threats to the system, define penalties for violations of the policy, and provide a policy updating mechanism.

Forcht and Ayers [2001] propose that an ISS policy should contain the following elements: scope, definitions, risk profile, requirements, security measures, disaster recovery procedures, internet security, application of policy, and coordinator's identification.

In the face of the diversity of proposals for ISS policy components, Höne and Eloff [2002a] undertook a comparison of several ISS international standards and gathered the key elements of an ISS policy as listed in Table 1.

Table 1. ISS Policies Components
Adapted from Höne and Eloff [2002a]

Components of an ISS Policy	
– ISS Need and Scope	– Roles and Responsibilities
– ISS Goals	– ISS Policy Violation and Disciplinary Action
– ISS Definition	– Monitoring and Review
– ISS Management Commitment	– User Declaration and Acknowledgement
– ISS Policy Approval	– Cross References
– ISS Policy Purpose	– General Elements (authors, date, review date)
– ISS Principles	

3. RESEARCH PURPOSE

As mentioned in the introduction, there is a lack of empirical studies in ISS policies. Despite the frequent criticisms of the lack of research on ISS policies and the inexistence of empirical studies in this area, we can observe, from the literature review, some difficulties to invert this situation.

In the sequence of this observation, this work aims to contribute to fill that gap, seeking to develop research which takes those criticisms into account, especially as far as the conduction of empirical studies and the contextualization of security policies application are concerned.

Thus, we intend to quantify ISS policies adoption by organizations. Faced with the diversity and dimension of the potential target sectors of this analysis, we chose to focus our attention on Public Administration, one of main investors in IT [Gartner 2009] and a sector which is in the interest of a high

number of constituents, in other words, all citizens. Hence, the purpose of this study was to characterize the current adoption of ISS policies by Portuguese City Councils.

4. SURVEY

In order to characterize empirically the adoption of ISS policies by Portuguese City Councils, a survey was thought to be the appropriate technique to apply, as it enables a clear, direct and objective answer to the questions presented to respondents. Besides this, since the aim was a complete characterization of the population, made up of 308 City Councils, this number was thought to make the use of alternative research techniques impossible or inadvisable.

As the survey focused on ISS policies, it became of central importance to adopt a definition which might be easily transmitted and understood by the respondents. Therefore, we chose to adopt the definition used by de Sá-Soares [2005, p. 56], for whom ISS policies are "documents which guide or regulate people or systems actions in the domain of information systems security". This is a sufficiently broad definition that does not preclude the possibility of City Councils having policy documents of different natures or with different structures, as previously discussed in subsection 2.2.

4.1 Population

The object of study of this work is Local Public Administration in Portugal, which is organized in 308 City Councils.

Among the 308 City Councils targeted in the survey, 308 questionnaires were carried out, which corresponds to a response rate of 100%. The survey was conducted to the whole population instead of using a random sample, enabling the collection of data about the whole population.

From the 308 contacts made, 299 were answered by phone and six by email after a previous phone call.

The respondents to this survey were the people in charge of IS in municipalities.

In order to standardize the questioning and the explanations provided to eventual requests for clarification by the respondents, the phone calls were undertaken by one of the authors, who strived to maintain a common discourse along the contacts so that potential influences on respondents' answers could be minimized. A brief explanation of the study was also prepared and transmitted to all the respondents on the initial stages of the phone interaction.

4.2 Structure

The survey structure was a result of the ISS policies literature review. The questions in the survey were organized in four groups.

The first group aimed to obtain a short characterization of both the City Council and the respondent, followed by groups of questions concerning ISS policies general features, which were preceded by the fundamental question: "Does the City Council have an ISS policy?".

Following the main question and in case the answer was negative, the respondents answered the group of questions in which they were asked whether they were planning to formulate a security policy, since they didn't have any. In case they were planning to do so, they were asked if the policy was already being prepared. When they were not thinking of formulating a security policy, they were asked about whether their option was due to the fact that they did not consider ISS an important matter.

When the answer to the main question was positive, the respondents answered the groups of questions focusing on policies as a product and on their formulation and implementation processes.

With respect to policies as a product, the questions were related to the way they are presented; what they include; their size in number of pages; who knows about the policy; where it is available; whether the roles, responsibilities and penalties for its non-compliance are defined; and whether the users have signed a statement of acceptance of the policy.

As far as processes are concerned, the questions were related to the policies timeline; who started the formulation process; who developed the policy; whether it was approved by superiors; who implemented it

and who supervises its enforcement; whether it was well accepted by its users; whether it is in force; whether it is reviewed; if there is one or many; and who it targets.

One last question asked to the respondents was related to the existence and identification of other information protection countermeasures.

4.3 Results

The main question in the survey aimed to find out about the existence of ISS policies in City Councils in Portugal.

As we can see in the chart in Figure 1, among the 308 City Councils, 38 (12%) stated that they have adopted ISS policies and 270 (88%) indicated that they have not adopted any policy.

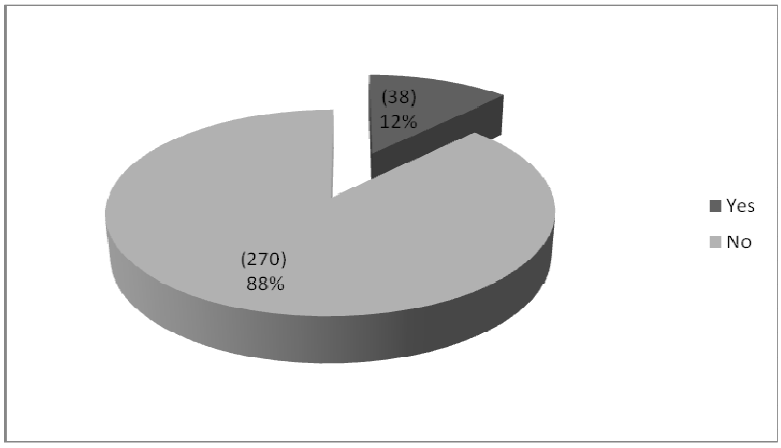

Figure 1. Adoption of ISS Policies

If we cross these answers with the respective City Council electoral dimension, we notice that among the 38 City Councils having ISS policies, 20 (52.6%) belong to "Medium Sized Municipalities" category, 9 (23.7%) to "Small Municipalities", 6 (15.8%) to "Large Municipalities" and 3 (7.9%) to "Very Large Municipalities". These percentages can be recalculated considering the number of City Councils included in each of those four categories, obtaining the distribution presented in Table 2.

Table 2. Distribution according to Electoral Dimension

Municipalities Categories	Number of Electors	Number of City Councils	Number of City Councils with Policies	%
Very Large	More than 100.000	20	3	15
Large	50.000 to 100.000	21	6	29
Medium Sized	10.000 to 50.000	150	20	13
Small	Up to 10.000	117	9	8

In relative values, we observe that the "Large Municipalities" category is the one which has the highest number of policies, followed by the "Very Large Municipalities", and with approximate figures the "Medium Sized Municipalities". "Small Municipalities" is the category with the lowest number of adopted policies.

The size of policies, in terms of their of number of pages, varies a lot in the universe of the 38 City Councils, the average being of eight pages per document, between a maximum of 30 pages and a minimum of one page.

Among the 38 City Councils having policies, 92% (35) have policies in which the users' roles and responsibilities are defined, whereas in the remaining 8% (3) such definition does not exist. In all of the 38 City Councils, the policies are known both by leaders and workers, without having been publicized among citizens, and are available internally in 97% (37) of the cases, and both internally and publicly in 3% (1).

Penalties definition for non-compliance with policy is not provided in 63% (24) of the City Councils. The respondents have justified such inexistence by saying that workers obey the laws applied to civil service, thus

being subject to disciplinary action irrespective of the existence or not of a defined penalty in the security policy document.

The initiative to develop the ISS policy is clearly taken by City Councils' IT managers/experts. The same happens with the responsibility for its formulation, implementation and enforcement.

The ISS policies apply to people in 61% (23) of the cases, to people and technology in 37% (14) of the cases, and only to technology in the remaining 3% (1) of the cases. Data gathered in the categories of application can be observed in the chart in Figure 2.

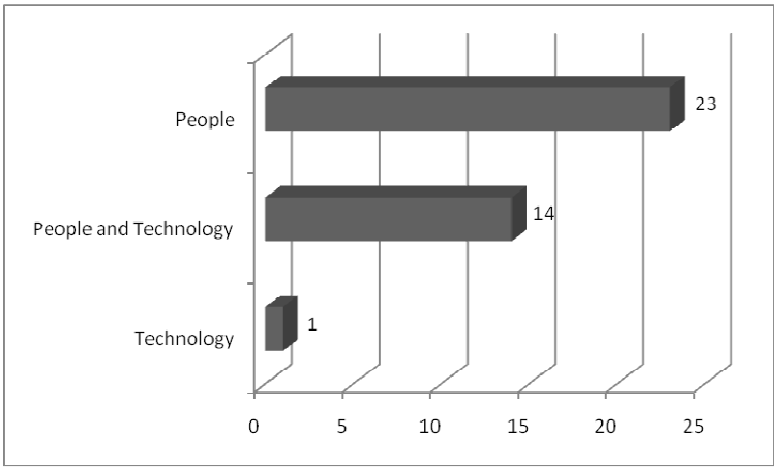

Figure 2. Application of ISS Policy

When questioned about the existence of one or more ISS policies, 89% (34) of the City Councils having policies said to have one global policy and 11% (4) said to have several partial policies.

As far as their acceptance is concerned, policies have been marked as well-accepted by workers in 79% (30) of the City Councils.

Although the majority of City Councils do not have an ISS policy, there were many in which it was said that they were thinking of formulating an ISS policy. More specifically, 66 % (177) of the respondents are considering the creation of an ISS policy, against 34% (93) which are not planning to formulate any policy.

Among the respondents who are planning to adopt an ISS policy, 42% (75) are already in the formulation process, whereas the remaining 58% (102) are willing to create a policy, but have not started the formulation process yet.

ISS policies are being enforced in the 38 City Councils that have adopted such a document. Three years is the average of the number of years for which the policies have existed in the sum of the 38 City Councils which gave a positive answer to the question related to the existence of a policy.

Finally, the existence of IS/IT protection mechanisms is a reality in all the City Councils. The most commonly used countermeasure is antivirus software. There are also firewall devices in many municipalities. Anti-spam filters and daily information backups are also widely used.

5. DISCUSSION

Although the majority of City Councils do not have an ISS policy, there were many in which a positive answer was given to the question about whether or not they were considering the formulation of an ISS policy. According to the information obtained from telephone contacts, this is mainly due to the present need to certify their services, under Quality Certification (ISO 9001), and to the adherence to digital cities networks projects in Portugal. It seems, therefore, that in many cases, the ISS policies adoption is based on a reactive process via factors which are exogenous to City Councils and related to certification and participation in regional computerization projects.

Based on these results, we can observe that 66% (177) of the respondents not having ISS policies are thinking of adopting one, whereas 34% (93) are not planning to formulate any policy. In the light of this

answer, these 93 respondents were asked about whether or not they consider ISS a matter of concern. The answer was invariably positive, in other words, although the respondents are not planning to formulate a policy, they consider ISS a matter of concern, justified by the value they admit information has. In an attempt to find an explanation for this incongruity, the respondents gave some explanations based on the fact that they used several ISS safeguards, thus not needing, in their view, an ISS policy in the form of a written statement.

The average of the number of years of existence of the policy in the total of the 38 City Councils is only three years. This suggests that sensitiveness towards the adoption of ISS policies is a recent thing.

One of the starting difficulties faced in the conduction of the survey was related to a lack of a clear and universal understanding about the ISS policy concept by the respondents. It was not without some difficulty that several respondents associated this concept with the set of security rules which establish the use of municipalities IS. One thing that might contribute to this is the huge profusion of formal "covers" to procedure norms and rules existent in City Councils, turned into a disparity of written documents, such as internal regulations, norms, orders, and even notices in the working place.

With respect to the components used in policies, we observe that among the 38 City Councils having an ISS policy, 37 have defined users' roles and responsibilities. The definition of penalties for disobedience to the policy only exists in 14 cases. The signature of a statement of acceptance of the policy is carried out in 17 cases.

The policy approval was carried out in 31 City Councils by its Leading Team, in five by the alderman and in two by the Municipal Assembly. As far as the policy enforcement is concerned, this task is done by the City Council IT department in 36 cases.

With respect to the reviews done to the policy, 33 respondents with policies have never done any review, two did one review, and two are due to do an annual review to the policy.

In the light of the study and the universe considered, we observe a difference between what is claimed in literature and what is seen in practice. Although authors such as Baskerville and Siponen [2002, p. 337] claim that it is "very consensual that a good information security policy is the basis for organizations information security", the respondents do not seem to be sufficiently alert or convinced of the foundation of this argument.

Whitman and Mattord [2005] indicate that security policies are the cheapest measures to formulate, but the most difficult to implement properly. We wonder whether respondents see the difficulties in the concrete application of ISS policies as one of the obstacles to their adoption. It is possible that the problem resides in a higher level, namely in the lack of a model for the ISS policies formulation, containing a clear indication of its features and components, adapted to the Local Public Administration organizational and institutional reality.

6. CONCLUSION

This study was based on the conduction of a survey to the 308 City Councils in Portugal, having reached a response rate of 100%.

The aim of this work was to try to contribute to the knowledge of reality in Portugal as far as ISS policies adoption is concerned, as well as to the enrichment of ISS literature, which lacks empirical studies.

The results of this study raise several interrogations, based on the low level of ISS policies adoption by Municipalities in Portugal. In order to plan the subsequent research, we propose that the works are organized around the analysis of four organization clusters. The 308 City Councils are thus distributed as follows: *Cluster* 1 – City Councils having an ISS policy (38); *Cluster* 2 – City councils which do not have an ISS policy, but are in a process of formulation (75); *Cluster* 3 – City Councils which do not have an ISS policy, but are planning to adopt one (102) and *Cluster* 4 – City Councils which do not have an ISS policy and do not intend to adopt one (93).

Among the future works to be done, we highlight the identification of facilitating and inhibiting factors to the adoption of ISS policies by City Councils, the proposal of a generic format for ISS policies to be adopted by City Councils and the proposal of a framework which may help Municipalities to formulate and implement ISS policies. We also intend to monitor the evolution of ISS policies adoption by Portuguese City Councils through the promotion of periodic surveys similar to the one described in this paper.

REFERENCES

Barman, S., 2001. *Writing Information Security Policies*. New Riders, Indianapolis.

Baskerville, R. and Siponen M., 2002. An information security meta-policy for emergent organizations. *Logistics Information Management*, Vol. 15, No. 5/6, pp. 337-346.

Bretschneider, S., 1990. Management Information Systems in Public and Private Organizations: An Empirical Test. *The Public Administration Review*, Vol. 50, No. 5, pp. 536-545.

Dhillon, G. and Backhouse J., 1997. Managing for secure organizations: a critique of information systems security research approaches. Technical Report, London School of Economics, Computer Security Research Centre, London.

Dhillon, G and Backhouse, J., 2000. Information System Security Management in the New Millennium. *Communications of ACM*, Vol. 43, No. 7, pp. 125-128.

Forcht, K. and Ayers, W., 2001. Developing a Computer Security Policy for Organizational Use and Implementation. *Journal of Computer Information Systems*; Vol. 41, No. 2, pp. 52-57.

Fulford, H. and Doherty, N. F., 2003. The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security*, Vol. 11, No. 3, pp. 106-114.

Gartner, 2009. *Dataquest Alert: Forecast, IT Spending in Industries, Worldwide, 3Q09 Update*. October.

Higgins, H. N., 1999. Corporate system security: towards an integrated management approach. *Information Management & Computer Security*, Vol. 7, No. 5, pp. 217-222.

Höne, K. and Eloff, J., 2002a. Information security policy — what do international information security standards say?. *Computers & Security*, Vol. 21, No. 5, pp. 402-409.

Höne, K. and Eloff, J., 2002b. What makes an effective security policy?. *Network Security*, Vol. 6, No. 1, pp. 14-16.

Hong, K.S. et al, 2003. An integrated system theory of information security management. *Information Management & Computer Security*, Vol. 11, No. 5, pp. 243-248.

JISC, 2001. *Developing an Information Security Policy*. Joint Information Systems Committee (JISC).

Kee, C., 2001. *Security Policy Roadmap – Process for Creating Security Policies*, SANS Institute.

King, C. M. et al, 2001. *Security Architecture: Design, Deployment, and Operations*. Osborne/McGraw-Hill, Berkeley.

Knapp, K. et al, 2006. Information Security: Management's Effect on Culture and Policy, *Information Management & Computer Security*, Vol. 11, No. 1, pp. 24-36.

Kotulic, A. and Clark, J., 2004. Why there aren't more information security research studies, *Information & Management*, Vol. 41, No. 5, pp. 597-607.

Lee, D., 2001. *Developing Effective Information Systems Security Policies*, SANS Institute.

Lindup, K. R., 1995. A New Model for Information Security Policies. *Computers & Security*, Vol. 14, No. 8, pp. 691-695.

Newcomer, K. E. and Caudle, S. L., 1991. Evaluating Public Sector Information Systems: More than Meets the Eye. *The Public Administration Review*, Vol. 51, No. 5, pp. 377-384.

OSIC and UMIC, 2004. *Inquérito à Utilização das Tecnologias da Informação e da Comunicação nas Câmaras Municipais 2004*, Observatório da Sociedade da Informação e do Conhecimento and Agência para a Sociedade do Conhecimento, Lisboa, Portugal.

OSIC and UMIC, 2006. *Inquérito à Utilização das Tecnologias da Informação e da Comunicação nas Câmaras Municipais 2006*, Observatório da Sociedade da Informação e do Conhecimento and Agência para a Sociedade do Conhecimento, Lisboa, Portugal.

Peltier, T. R., 2002. *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Auerbach Publications, Boca Raton.

de Sá-Soares, F., 2005. *Interpretação da Segurança de Sistemas de Informação Segundo a Teoria da Acção*, PhD Thesis in Information Systems and Technologies, Universidade do Minho, Guimarães.

Schneier, B., 2000. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, New York.

Shorten, B., 2004. Information Security Policies from the Ground Up. In Tipton, H. F. and Krause, M. (Eds.), *Information Security Management Handbook* (Fifth ed.), Auerbach, Boca Raton, pp. 917-924.

Whitman, M. E., 2004. In defense of the realm: Understanding threats to information security. *Informational Journal of Information Management*, Vol. 24, pp. 3-4.

Whitman, M. and Mattord, H., 2005. *Principles of Information Security* (Second ed.), Course Technology, Boston.

Whitman, M. et al, 2001. Information Systems Security and the Need for Policy, In Dhillon, G. (Ed.), *Information Security Management: Global Challenges in the New Millennium*, Idea Group Publishing.

Wood, C. C., 1995. Writing InfoSec Policies. *Computers & Security*, Vol. 14, No. 8, pp. 667-674.