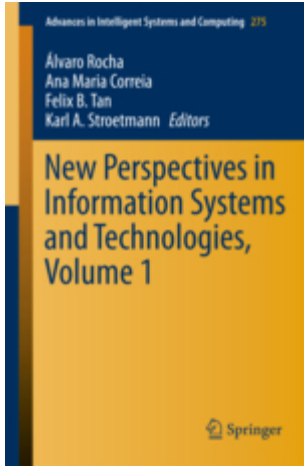
Advances in Intelligent Systems and Computing 275
Álvaro Rocha
Ana Maria Correia
Felix B. Tan
Karl A. Stroetmann Editors
New Perspectives in Information Systems and Technologies, Volume 1
Springer

Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises

Isabel Lopes and Pedro Oliveira

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

Abstract. Information security is a relevant fact for current organizations. There are factors inextricably linked to this issue, and one cannot talk about information security in an organization without addressing and understanding the information security culture of that institution. Maximizing the organizational culture within an organization will enable the safeguard of information security. For that, we need to understand which the inhibiting and the enabling factors are. This paper contributes to point out those factors by presenting the results of a survey concerning information security culture in small and medium sized enterprises (SMEs). We discuss the results in the light of related literature, and we identify future works aiming to enhance information security within organizations.

Keywords: Security Culture, Information Security, Small and Medium Sized Enterprises, Information Security Culture.

1 Introduction

One of the major benefits of the creation of an information security culture is the protection of the organization assets in which will have "direct interaction with information assets and thereby minimize the threats that user behaviour poses to the protection of information assets" [1] (p.1). The importance of creating a security culture within organization settings arises from the fact that the human dimension in information security is always considered to be the weakest link [2]; [3]; [4]; [5]; [6]. Therefore, the creation of an information security culture is necessary for effective information security management [7]. Within the scope of this paper, a review of literature on security culture was done. Although there is a high number of works concerning security culture, there seem to be no agreement on the meaning of this term. Therefore, we proceed to present some concepts in order to help frame and understand this study:

- The author [8] defines security culture as: the whole of human attributes, such as behaviors, attitudes and values which may contribute to the protection of all kinds of information within a certain organization.
- Another author [9] claims that security culture reflects the attitudes, beliefs, perceptions and values that employees share as far as security is concerned.

Á. Rocha et al. (eds.), *New Perspectives in Information Systems and Technologies, Volume 1*, Advances in Intelligent Systems and Computing 275,
DOI: 10.1007/978-3-319-05951-8_27,

- For [10], security culture consists of attitudes, beliefs and perceptions shared by the members of the group, who define norms and values which, in turn, determine the way they act and react regarding risk and the risk control system.

The definitions listed are clear with respect to the definition of security culture, and although they mention different aspects, they are consensual in some respects, namely when considering security culture as values and beliefs.

In this work, we consider that beyond the beliefs, values and behaviors of executives and workers regarding information security, security culture is also a policy that must be conducted according to the mission of the organization with a focus on information security.

There is another term closely related to security culture: organizational culture. This concept holds a more subjective aspect, which at times makes it different within the organization itself.

This subjectivity, as well as the lack of agreement on what constitutes a security culture, represents a deadlock regarding the identification of the factors needed to create a security culture. This paper attempts to fill this gap by studying the enabling and inhibiting factors for the implementation of an information security culture within SMEs in Portugal.

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 approach the theoretical foundations guiding this study. 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 we propose future works.

2 The Importance of Information Security

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 as well as the 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 information security technical measures, but also and ever more organizational and social measures, as this is the only way to reach organizational well-being as well as to maintain organizations integrity [11].

Information security is a critical aspect for most organizations. The growing importance of information technology and the massive use of internet and its related services brought about an increasingly higher number of attacks which information is exposed to. Therefore, the need to protect information is urgent.

Information represents one of the current organizations main assets, and the systems which support that information are increasingly more exposed to threats. 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 [11], 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.

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 complexity. For [13], 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 Theoretical Foundations

Turning to organizations whose information assets are the least protected, experts suggest that small and medium sized enterprises (SME) are particularly disadvantaged in the development of secure employee behavior [13]; [14]; [15]; [16]. We suggest that developing a strong information security culture in SMEs may address many of the behavioral issues that underpin information security breaches in such companies.

Although all organizations have their own requirements as far as information security is concerned, SMEs offer one of the most interesting cases for studying the issue of information security in particular, and information security culture in general. Within the organizational universe in Portugal, SMEs assume a unique relevance due to their high number, which makes information security efficiency a crucial issue.

No company is immune to the effects of the revolution caused by information. They must be aware that information is an asset as valuable as human resources, since the success or failure of the daily decision-making within the organization depends on it.

For these reasons, this study aims to identify the enabling or inhibiting factors for the adoption of an information security culture within SMEs in Portugal. By doing so, we intend to give our contribution so that SMEs may over time have their assets more safeguarded.

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 348,552 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 less than or equal to 50 million Euros; and an annual balance-sheet total which must be less than 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 answer, 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 culture. 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.

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

5 Results

Among the 307 SMEs involved in this study, 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.

We tried to enquire the person in charge of the IT sector whenever possible, which happened in 57% of the cases.

When asked about who was responsible for the company's information technology, the answers showed that in most companies (52%) there is an internal department or a worker in charge, whereas in the remaining 48%, such responsibility belonged to external companies.

The main question of the survey aimed to provide information on the existence of an information security culture. In order to define and tell whether a company has an information security culture, we relied on the norm ISO IEC 27002:2005 [18], which defines 127 controls making up the endeavor of the Information Security Management System, grouped in 11 control sections: Security Policy; Organization of Information Security; Asset Management; Human Resources Security; Physical and Environmental Security; Communications and Operations Management; Access Control; Information Systems Acquisition, Development and Maintenance; Information Security Incident Management; Business Continuity Management; and Compliance.

We considered that a company adopts an information security culture whenever at least 5 of the above controls are adopted.

As shown in Fig.1, 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.

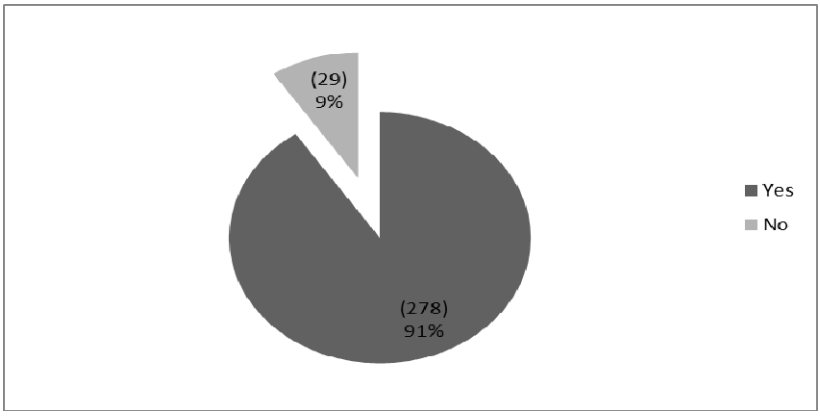

Fig. 1. Adoption of an information security culture

The cross-reference of this data with the distribution per number of workers in the respective company shows that among the 29 companies which have an information security culture, 2 are "Micro" enterprises; 10 are "Small" and 17 are "Medium sized". These numbers must be weighed up with the number of companies per type comprised in each of the three existing types. The results are presented in Table 2.

Table 2. Distribution per number of workers

Type de enterprise	N. of Workers	N. of enterprises	N. of enterprises surveyed	N. of enterprises with a security culture	%
Micro	1-9	329,730	100	2	2
Small	10-49	16,381	90	10	11
Medium sized	50-249	2,439	117	17	15

Overall, the data shows that "Medium sized" enterprises are the ones possessing a higher number of policies, closely followed in numbers by the "Small" enterprises. "Micro" enterprises, which largely differ from the others as far as their number in Portugal is concerned, showed to be the ones adopting the fewest information systems security cultures.

Among the respondents who reported not to have an information security culture in their company, 151 (54%) are not planning to adopt information security measures. However, and although this may seem contradictory, when questioned about whether they consider information security important, they unanimously reported to considered it very important.

The remaining 127 (46%) respondents who do not have an information security culture in their company are planning to implement information security measures. The measures they are thinking of adopting range from information systems security policies to higher investments in IT and software which safeguards the company's information. In 30% of the cases, tenders were or are being conducted viewing the acquisition of such means.

Within the 29 companies which adopt an information security culture, the kinds of measure implemented are as presented in the chart below.

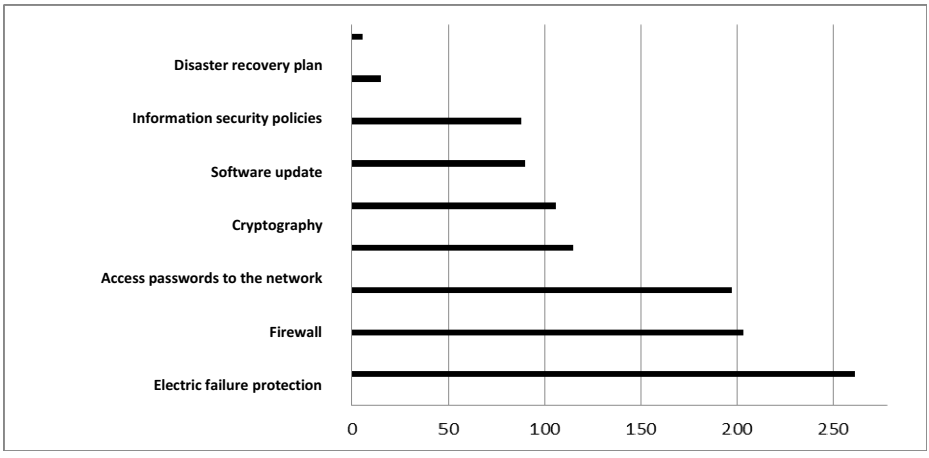

Fig. 2. Adopted information security measures

The data presented in the chart shows that the measures taken in a largest scale are those related to physical equipment, followed by those linked to the logical layer, and finally by those associated with the human aspect of the company, which is the one presenting the highest lack of concern from the company and its leaders. It is important to highlight that many of the measures within the human layer are not difficult to implement and require, in most cases, low investments from the executive board either in IT tools or in time and dedication.

With regard to which factors may be considered enabling for an information security culture, the results obtained assume various natures and can be grouped as follows:

Political
- Defining the goals for security
- Having the board's approval
- Being acknowledged by all users

Human
- Qualified workers
- Users' training
- Compliance monitoring
- Commitment towards implementation
- Users understanding of the advantages
- Technicians' training

Technological
- ICT Acquisition

On the other hand, the results of this analysis show that the inhibiting factors for an information security culture in a SME can be grouped into the following categories:

Political
- The non-approval of measures

Human
- Lack of time and of human resources
- Users resilience
- Users' disobedience

Technological
- Satisfaction towards the ICT currently used
- The existence of enough technology to ensure security

Among the inhibiting factors for the adoption of an information security culture, we highlight two: users' resilience and users' disobedience. Resistance to change is always high when users' work routines are altered, and the adoption of measures is no exception. Thus, converting mere recommendations into compulsory normative acts which include the adoption of restrictions for those who do not comply with the rules defined may turn into a strong inhibitor for the implementation of actual information security measures. Therefore, such measures should be complemented with a strong

investment both in the promotion of the importance of complying with the security rules and in users' training.

Finally, the existence of other information protection mechanisms is a reality in most companies. The protection mechanism most commonly used is the anti-virus software. Firewalls also exist in high numbers, and anti-spam filters and backups are also widely used.

Organizational culture is composed of guidelines and values concerning security which enable the implementation of a security culture. Defining a policy as well as the goals for security may be an indicator that there is a commitment towards a security culture. The security culture must be build up from the executive board, as this is where the organization's central values are defined. Meanwhile, the main indicator is the behavior of all its cooperators within their daily activities.

In other words, it is necessary to consider not only the technical aspects but also and ever more the organizational, human and social aspects, as only this will enable organizational well-being.

6 Conclusion

Despite the crucial role played by organizational culture in determining an organization's success or failure, there seem to be no consensus regarding the description of organization culture [18]. Each organization has a culture (or perhaps a set of subcultures) and such culture may have an effect on security. Understanding how this happens may provide insights on possible ways to change organizational cultures so that security is given higher priority.

The SMEs under analysis are open systems, which means that they interact with the outside environment within which they are located, receiving trends and being influenced. Similarly, the individuals working in those organizations also take part in that same interaction process. In the light of this, we perceive the existence of various cultures within the same organization.

For some authors, each organization has a security culture of some kind, which may be described as strong or weak, as positive or negative. For other authors, only an organization which has a strong commitment towards security may be said to have a security culture. From this point of view, relatively few organizations have security policies.

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.

Companies must clearly define their strategic goals and identify their culture's characteristics, boosting the areas which enhance the intended results and reinforcing the ones which are less developed. Acknowledging the characteristics of the organizational culture and committing towards the achievement of the strategic goals is not the responsibility of the leadership only, but of all the company's workers.

Among future works which can be conducted, we highlight the extension of the scope of this study towards large enterprises 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. Da Veiga, A.: Cultivating and Assessing Information Security Culture. University of Pretoria (2008)
2. Da Veiga, A., Eloff, J.H.P.: Information security culture – validation of an assessmentinstrument. Information Systems Management 24, 361–372 (2007)
3. Martins, A., Eloff, J.H.P.: Information Security Culture. Paper presented at the 17th International Conference on Information Security (2002)
4. Maynard, S., Ruighaver, A.B.: Evaluating IS Security Policy Development. Paper presented at the Third Australian Information Warfare and Security Conference, Perth, Australia (2002)
5. Schlienger, T., Teufel, S.: Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. Paper presented at the DEXA Workshops (2003)
6. van Niekerk, J., von Solms, R.: A holistic framework for the fostering of an information security sub-culture in organizations. Paper presented at the 4th Annual ISSA Conference South Africa (2005)
7. Eloff, M.M., von Solms, S.H.: Information Security management: A Hierarchical Approach for various frameworks. Computer & Security 19(3), 243–256 (2000)
8. Dhillon, G.: Managing and controlling computer misuse. Information Management & Computer Security 7(4), 171–175 (1999)
9. Lee, T.: Assessment of safety culture at a nuclear reprocessing plant. Work & Stress 12(3), 217–237 (1998)
10. Hale, A.R.: Culture's confusions. Safety Science 34, 1–14 (2000)
11. Dhillon, G., Backhouse, J.: Information System Security Management in the New Millennium. Communications of ACM 43(7), 125–128 (2000)
12. Wood, C.C.: Writing InfoSec Policies, Computers & Security 14(8), 674–667 (1995)
13. Dimopoulos, V., Furnell, S.M., Jennex, M., Kritharas, I.: Approaches to IT Security in Small and Medium Enterprises. In: Proceedings of the 2nd Australian Information Security Management Conference 2004, Perth, Australia (2004)
14. Furnell, S.M., Gennatou, M., Dowland, P.S.: Promoting Security Awareness and Training within Small Organisations. In: Proceedings of the 1st Australian Information Security Management Workshop, Deakin University, Geelong (2000)
15. Helokunnas, T., Iivonen, I.: Information Security Culture in Small and Medium Size Enterprises. Seminar Presentation, Institute of Business Information Management, Tampere University of Technology, Finland (2003)
16. Taylor, M., Murphy, A.: SMEs and eBusiness. Journal of Small Business and Enterprise Development 11(3), 280–289 (2004)
17. ISO/IEC 27002, Information technology — Security techniques — Information security management systems — Requirements, International Organization for Standardization/ International Electrotechnical Commission (2005)
18. Guldenmund, F.W.: The nature of safety culture: a review of theory and research. Safety Science 34, 193–214 (2000)