Advances in Intelligent Systems and Computing 353

Álvaro Rocha
Ana Maria Correia
Sandra Costanzo
Luís Paulo Reis *Editors*

New Contributions in Information Systems and Technologies

Volume 1

Springer

Applying Action Research in the Formulation of Information Security Policies

Isabel Lopes and Pedro Oliveira

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

Abstract. Information Systems Security (ISS) is crucial in all and each of the services provided by organizations. This paper focuses on Small and Medium Sized Enterprises (SMEs) as 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 policies. Within the organizational universe, SMEs assume a unique relevance due to their high number, which makes information security efficiency a crucial issue. There are several measures which can be implemented in order to ensure the effective protection of information assets, among which the adoption of ISS policies stands out. This article aims to constitute an empirical study on the applicability of the Action Research (AR) method in information systems, more specifically through the formulation of an ISS policy in SMEs. The research question is to what extent this research method is adequate to reach the proposed goal. The results of the study suggest that AR is a promising means for the formulation of ISS policies.

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

1 Introduction

Security requirements change at a bewildering speed both in large and in SMEs. Companies manipulate increasingly more and larger quantities of information, which is why increasingly stricter and wider security controls are essential. The technological process can work as a catalyst of threats, but is not enough on its own to ensure information security.

Reaching the information security levels which are adequate to each organization is important, but similarly or even more important is to be able to maintain those levels. Having software and hardware which contribute to information security is not enough. Organizations also need a security policy as well as good security management in order to appropriately support the efforts to protect the information system assets.

By Information Systems Security (ISS) we mean the "organizational framework of culture, policies, organizational structures and operational environment used to ensure the integrity, availability and confidentiality of an organization's information" [1].

Á. Rocha et al. (eds.), *New Contributions in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 353, DOI: 10.1007/978-3-319-16486-1_50

In this paper, we adopted the definition of ISS policy proposed by [2], for whom ISS policies are "documents which guide or regulate people or systems' actions in the domain of information systems security".

Although there is a considerable agreement in literature regarding the main role played by ISS policies, there is evidence that organizations often fail in the formulation of this security control. When focusing our attention on a specific type of organization, SMEs, a study carried out by [3] 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.

This article aims to constitute an empirical study on the applicability of the Action Research (AR) method in information systems, through the adaptation of an ISS policy model proposed by the researcher to each of the 10 companies which constitute the universe of this study.

This study was carried out "in loco" within 10 SMEs which had not yet adopted an ISS policy and which had pointed out the non-existence of an ISS policy model which they could adapt to their company as the main inhibiting factor for the adoption of such a policy.

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

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, including the security of their information assets.

Structurally, this paper is organized as follows. After this introduction which contextualizes the study, we point out some concepts and descriptions, namely regarding the formulation of ISS policies and the AR method. Afterwards, we describe the cooperation efforts which were promoted towards the formulation of ISS policies within 10 SMEs in Portugal. Such description is followed by a discussion, and finally, we enumerate the papers' main contribution, limitations, and suggestions for future works.

2 Formulation of an ISS Policy

In order to adopt an ISS policy, an organization must follow a sequence of steps, starting by writing the policy, then implementing it, and later on, at predefined moments or whenever circumstances require it, by reviewing its provisions, which may prompt modifications in the policy. Indeed, this sequence of steps may be viewed as a cycle (Figure 1) [3].

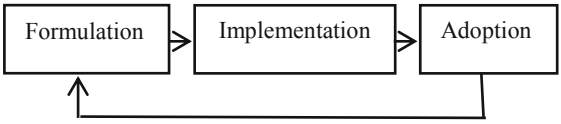

Fig. 1. The security policy application process

The ISS policy is considered to be vital within an organizational strategy. However, in order to make IS secure, authors such as [4] claim that it is not always easy to write such a document. Actually, the authors of such documents often make use of commercial sources or minutes which are available, and make copies of these documents, which therefore do not reflect the true culture of the organization, thus not resulting in an effective document regarding ISS.

Writing an ISS policy is an essential component for all successful information security efforts. The policies establish the stage for a wide variety of information security efforts [5]. However, the formulation of such a policy is not a straightforward task and depends on a variety of factors.

The formulation of a policy takes place at a planning stage, in most cases as part of a wider security plan which aims to provide adequate protection to IS through a set of security measures and practices [6].

Although there are several contributions which provide guidelines to the formulation of an ISS policy (norms for security management, best practices, etc.), the formulation process represents a very demanding and considerably complex task.

In figure 2, we present a process of ISS policy formulation [7]. This process includes input elements which feed certain activity processes which, in turn, will originate a set of outputs.

The formulation process of an ISS policy, which ultimately results in the security policies document, involves a complex series of studies, analysis and compilation of a significant number of elements.

The process of security policy formulation (Input) uses, among others, the result of risk assessment and the guidelines for security management standards and best practices as an entry.

The process of security policy formulation (Activities) uses a set of activities such as compiling the security policy document, writing the security procedures, and compiling the specifications for technical security controls.

Input	Activities	Output
• Results of the risk evaluation assessment • Legal requirements • Information on the structure and cultural characteristics of the organization • Existing security practices • Knowledge of information technology and security controls • Guidelines for security management standards and best practice	• Identify security requirements for the information systems • Identify required security controls • Compile security policy document • Write down security procedures • Compile the specifications for technical security controls	• Security policy for information systems • Specification for countermeasures

Fig. 2. The process of security policy formulation

The process of security policy formulation (Output) consists of the resulting ISS policy document as well as of the specifications to be taken into account during possible adjustments.

As mentioned above when listing the characteristics of ISS policies, it is within the formulation process that efforts must be undertaken in order to conceive policies which have clear goals, guidelines and procedures. Also, it is important to consider the inclusion of a well-defined "exception to the rule" provision, which will provide the policy with a certain level of flexibility which will be needed if circumstances so require [8].

Besides what has been said regarding the ISS policy formulation process, it is crucial to know that there is not only one unique method to develop an ISS policy. Factors as diverse as the target audience, the kind of business, the size of the company or the possible existence of an ISS policy play an important role in influencing the ISS policies formulation process [9].

3 Perspectives on Action Research

In a nutshell, we can say that AR is a research methodology oriented towards practice improvement regarding the various fields of action [14]. Therefore, the basic and essential twofold goal consists of obtaining better results in what we do and enhancing the refinement of both the people and the groups that we work with.

As its name suggests, Action Research is a methodology which has a twofold objective of action and research, as it intends to obtain results in both areas:

- Action – the aim is to reach change within a community, organization or program;
- Research – by increasing understanding by the practitioner, client or community [10].

The AR method executes an iterative cycle composed of a series of steps, whose numbers and designations vary depending on the authors. The author [11] present a model adapted from Dick (1992) which includes three steps: Planning; Action; and Reflection, as presented in Figure 3.

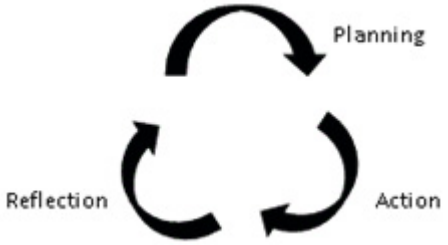

Fig. 3. Three steps AR cycle

Based on these three building blocks, [12] summarize the philosophy underlying AR: "You plan an intervention (Planning); you execute the corresponding action (Action), thus inducing a change which will hopefully lead to some development; finally, you do a critical analysis of the results, which supposedly leads to a better knowledge of the situation. This, in turn, enables you to make adjustments leading to new cycles (Reflection)."

Numerous models are presented in literature, but these three stages of the cycle seem to be present in almost all of them, thus representing the basis for other AR models.

This is the model which is going to be followed within this study, as we consider it to be sufficient and effective to the achievement of the proposed goals.

Therefore, we can say that AR is a dynamic methodology, as it is a research and action cyclic process. Whenever conditions are not the desirable ones, a new cycle is started, a new planning is made and a new process takes place.

4 Action Research Applied to the Formulation of ISS Policies

One of the main reasons pointed out to justify the use of qualitative research methods in the field of IS is the fact that Information Systems include the human element as a variable or as a determining research factor, whether the study focuses on the individual or on the group, as in the case of organizations or companies.

Thus, AR constitutes "one of the few research approaches which we can legitimately use to study the effects of specific changes in methods of systems development within human organizations." [13].

For these reasons, it is understandable that the application of AR suits the study of formulating ISS policies in SMEs.

The adoption of an ISS policy follows a complex life cycle from its formulation to its implementation and finally its adoption (Figure 1). This study focuses on the formulation stage of an ISS policy within 10 SMEs.

The drafting of an ISS policy primarily requires an acknowledgement of its features and components. We first collected that information and then wrote the document which was adapted on-site to each one of the 10 companies. After this, a final version of the document was written in a joint work by the researcher and the element within each company who was more closely involved in the process. The following aspects were taken into account for the drafting of that first document.

The first thing to be considered when writing a policy is to use language that is easy to understand and not to make it too complicated. According to author [14], policies should be written using the SMART rule (**S**pecific, **M**easurable, **A**greeable, **R**ealistic and **T**ime-bound).

Although it is widely accepted that an ISS policy can vary significantly from organization to organization, the author [5] claims that such a document must typically include the following elements: general statements of aims, goals, beliefs and responsibilities, which are often accompanied by general procedures for achieving them.

Another author, [15] states that a good ISS policy should outline individual responsibilities, define which users are authorized or not to use the system, provide workers with reports on possible threats to the system, define sanctions for possible violations of the policy, and provide an update mechanism for the policy.

More components could be listed here, however, the ones mentioned above are considered to be sufficient as this is not the particular focus of this work.

After drafting the first version of the document, we selected the companies where the joint formulation of the document and its subsequent implementation would take place.

Four essential aspects were taken into account for the selection of the SMEs:

1. The SMEs geographic location;
2. Their dimension;
3. The fact that they did not have an implemented ISS policy;
4. The fact that they did not know how to formulate an ISS policy.

With regard to the first point, and considering that AR is a participatory research method which requires some time spend on-site in each one of the companies, we limited its implementation to one district in Portugal.

As far as the company dimension is concerned, and bearing in mind that SMEs are composed of Micro, Small and Medium Sized companies, we tried to cover the three types, thus selecting some Micro (1), Small (3) and Medium Sized (6) companies.

Another aspect taken into account was the fact that the companies did not have an implemented ISS policy.

Finally, we only selected companies which pointed out the difficulty in drafting a document as an inhibiting factor for not having implemented an ISS policy before.

After selecting the companies and drafting a first version of the ISS policy, we moved on to the next stage, contacting directly with the head of the IT department (8 cases) and with the owner of the company (2 cases).

The process of formulating an ISS policy in these companies matched the AR cyclic model presented in Figure 3, which is composed of three steps: Planning, Action and Reflection.

As far as the planning step is concerned, the first stage starts with the detection of the problem. It is strongly advisable that the problem is identified and formulated objectively and in a way that allows intervention. Therefore, we present in Figure 5 a depiction of this first stage.

Problem
Difficulty in formulating an ISS policy; Not having an ISS policy
Significant data
A study carried out within a universe of 307 SMEs concluded that only 15 companies had an ISS policy; Among these 307, 122 (40%) pointed out that one of the inhibiting factors for the non-implementation of a policy was its formulation
Desirable conditions
Formulation of a model of ISS policy which can be adopted by as many companies as possible; That the implementation of an ISS policy becomes a reality in SMEs in Portugal.

Fig. 4. Identification of the problem

Besides identifying the problem, it was necessary to define the project and develop the mediation process. In order to achieve this, a thorough study of the company had to be carried out at this stage, including an analysis of the company's information system users and technological resources, namely concerning the existence of antiviruses, firewalls and IT equipment in general.

Within the second step of the AR cycle – Action – we specified the actions which would have to be undertaken so that the ISS policy could be definitively written, or in other words, so that the ISS policy could be formulated. Such actions were defined in a joint work between the researcher and the person who was accompanying the process in each of the ten companies. This process started with the analysis of the document presented by the researcher as far as its applicability to that particular company was concerned.

The actions to be undertaken regarded the study of the components and features that needed to be removed, altered or added. This task took into account the fact that all companies are different and that the document must reflect the true culture of the organization always aiming towards an effective security of its information systems.

The actions to be implemented were undertaken and a final drafting of the document took place, always with the contribution of the member of the company linked to this study. These actions were executed with the aim to lead to a change within the organization. This step involved three stages: firstly, the analysis of the ISS policy model provided by the researcher; secondly, the final drafting of the ISS policy document and its further approval; finally, the implementation of the ISS policy within the company.

In the third step of AR methodology – Reflection – the aim is to assess whether or not the goals were achieved and whether or not the problems were solved. In this respect, it is important to understand that the formulation of the ISS policy document does not alone imply that the company has an ISS policy, which means that the

problem is not solved. Therefore, a second cycle must be conducted in order to develop an implementation process which includes all the stages intrinsically connected to it.

5 Discussion

One of the aims of this work was the adoption and subsequent implementation of an ISS policy model by the 10 SMEs which constituted the universe of this study. However, above all, we intended to help these SMEs change a concrete situation, which was the non-adoption of an ISS policy, as well as understand that situation and alter it.

The formulation of an ISS policy following the AR method was aimed at the construction of a solution to generate new knowledge useful to the participants on how to implement an ISS policy and improve its practice through successive evaluations and associated changes whenever necessary. Not only did the researchers cooperate in that process, but they also aimed to contribute to the existing knowledge, trying to understand the hindrances faced by organizations in the process of ISS policy adoption and to research on the effectiveness of initiatives put into practice to overcome those difficulties. By participating in several of those processes, the research team collected evidence that may prove to be useful for projecting future interventions in other organizations of the same type. This dual interest of researchers – helping to change the specific context of practice (Action) and adding to the general knowledge of the ISS policy adoption process (Research) – raises some questions. Since the intervention is based on a cooperative structure, and since the control over intervention by researchers is limited, the clear articulation and negotiation of the goals, views, and interests of the two groups of participants is particularly relevant.

Given the collaborative nature of this study, the insights of the participating researcher were often debated and brought to reflection in order to produce a shared understanding that led to change. Indeed, it was not intended that the researcher would unilaterally propose a change plan, but to build such a plan jointly with the other actors involved in the transformation. Therefore, the model initially proposed by the researchers was merely a prototype, which was altered and shaped to fit each one of the 10 SMEs in a further joint work with the companies.

Within the research method under study, the researcher interacts directly with the company, thus basing the research on a collaborative structure. Therefore, one of the main points of criticism is the researcher's inability to manipulate or control certain aspects, namely the articulation between their own goals, often more academic-related, with the company's goals.

During the present application of AR, these aspects were taken into account in an attempt to ensure more rigor and validity as well as less limitations regarding most of the conclusions drawn from the study. Whenever possible, an attempt was made not to manipulate or control neither the formulation of the policy nor the adoption and adaptation of the proposed model to the SME reality.

This research method allows the participants to obtain a very wide knowledge of the company, which enables the formulation of a policy which can fit perfectly into the reality of each SME. The integration of the ISS policies into the organizations'

goals, processes and culture is paramount to ensure the success of the policy formulation as well as of its further implementation.

An ISS policy must constitute a constructive and protective vehicle and not a mechanism that hinders the good development of the organization's work. Therefore, before formulating a policy, we must take into consideration the company's goals as well as its organizational processes and culture.

Although the factors mentioned above seem to be obvious and must be taken into account throughout the whole formulation process of an ISS policy, the ultimate bottom line for such policies is that they can truly be implemented. Also, it is important that such policies are concise and easy to read and understand in order to ensure their acceptance by users. Besides this, another important aspect to consider when formulating an ISS policy is its compliance with the legal system in force.

An ISS policy must include a set of directives, provisions and procedures which need to be obeyed and aim to raise users' awareness and guide them towards a secure use of technologies, providing them with information on how to manage, save and protect one of their main assets – information.

Over the last decades, either to a larger or to a smaller extent, organizations have become dependent on their information systems. Therefore, the value of information has assumed a vital importance to organizations worldwide, regardless of their size. The attention that was primarily given to their tangible and financial assets has now turned towards the information asset and, consequently, the security of this asset has started to be treated differently. Among the existing information security measures, particular emphasis should be placed on ISS policies. However, their institutionalization is not observed yet, namely within SMEs.

Therefore, the existence of a basic standard ISS policy model may represent a facilitator means to the institutionalization of an ISS policy in SMEs, thus helping to make the existence of ISS policies in SMEs in Portugal a reality.

6 Conclusions

The results of the study suggest that AR is a promising means for the institutionalization of ISS policies adoption. It can both act as a research method, improving the understanding among researchers about the issues that hinder such adoption, and as a change method, assisting practitioners to overcome barriers that have prevented the formulation of ISS policies in SMEs.

This research work presents limitations, namely with respect to the number of SMEs involved. Although we believe that the study carried out in the ten SMEs generated enough data to serve the goal of the study, we also believe that a larger number might result in a more sustained set of data. Nevertheless, we highlight that the application of the AR method requires the researcher's direct involvement, thus requiring a substantial amount of time.

Among the works which might be carried out in the future, we highlight the formulation of a proposal of an ISS policy model which is as flexible and comprehensive as possible and which may be adopted by as many SMEs as possible, in order to invert the reduced number of ISS policies found in these companies. Such a model should have the agreement of a national public umbrella organization

overseeing SMEs so that its distribution among SMEs can be swift. These proposals may reveal to be an important tool towards the institutionalization of ISS policies in SMEs.

References

1. Beatson, J.G.: Information Security: The Impact of End User Computing. In: Gable, G.G., Caelli, W.J. (eds.) IT Security: The Need for International Cooperation — Proceedings of the IFIP TC11 Eighth International Conference on Information Security, Amsterdam, pp. 35–45. Elsevier (1992)
2. de Sá-Soares, F.: Interpretação da Segurança de Sistemas de Informação Segundo a Teoria da Acção, PhD Thesis in Information Systems and Technologies, Universidade do Minho, Guimarães (2005)
3. Lopes, I., Oliveira, P.: Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises. In: Rocha, Á., Correia, A.M., Tan, F., Stroetmann, K. (eds.) New Perspectives in Information Systems and Technologies, Volume 1. AISC, vol. 275, pp. 277–286. Springer, Heidelberg (2014)
4. Höne, K., Eloff, J.: Information security policy — what do international information security standards say? Computers & Security 21(5), 402–409 (2012)
5. Wood, C.C.: Writing InfoSec Policies. Computers & Security 14(8), 667–674 (1995)
6. Peltier, T.R.: Information Security Policies. Procedure: a practitioner's reference. CRC Press (1999)
7. Karyda, M., Kiountouzis, E., Kokolakis, S.: Information systems security policies: a contextual perspective. Computers & Security 24(3), 246–260 (2005)
8. Wills, L.: Security Policies: Where to Begin. Security Essentials 1(4b) (2002)
9. Diver, S.: Information Security Policy – A Development Guide for Large and Small Companies. SANS Institute (2007)
10. Dick, B.: A beginner's guide to action research, Southern Cross University, Australia (2000), `http://www.scu.edu.au/schools/gcm/ar/arp/guide.html`
11. Cunha, P.R., Figueiredo, A.D.: Research and Critical Rationalism: a Virtuous Marriage. In: Proc. of the Xth European Conference on Information Systems (ECIS), Gdansk, Poland (2002)
12. Susman, G., Evered, R.: Na Assement of the Scientific Merits of Action Research. Administrative Science Quarterly 23(4), 582–603 (1978)
13. Baskerville, R., Wood-Harper, A.T.: A Critical Perspective on Action Research as Method for Information Systems Research. Journal of Information Technology 3(11), 235–246 (1996)
14. Kee, C.: Security Policy Roadmap – Process for Creating Security Policies. SANS Institute (2001)
15. Whitman: In defense of the realm: Understanding threats to information security. Informational Journal of Information Management 24, 3–4 (2004)