Advances in Intelligent Systems and Computing 445

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

New Advances in Information Systems and Technologies

Volume 2

Springer

The Security Policy Application Process: Action Research

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. It is crucial for companies to acknowledge the need for applying security policies because, without such policies, there is no reliable way to define, implement, and enforce a security plan within an organization. Small and medium sized enterprises (SME) are no exception. Within the organizational universe, SMEs assume a unique relevance due to their high number, which makes information security efficiency a paramount 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. A recent survey concluded that from 307 SMEs, only 15 indicated to have an ISS policy [1]. The conclusion drawn from that study was that the adoption of ISS policies has not become a reality yet. As an attempt to mitigate this fact, security policies were formulated, implemented and adopted in 10 SMEs which had stated not to have this security measure. These interventions were conceived as Action Research (AR) projects.

Keywords: Formulation, Implementation and Adoption of Information Security Policies, Information Security, Small and Medium Sized Enterprises.

1 Introduction

Security requirements change at a bewildering speed both in large companies 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 [1].

Information security encompasses technology, processes, and people. Technical measures such as passwords, biometrics, and firewalls alone are not sufficient in mitigating threats to information. A combination of measures is required to secure systems and protect information against harm [2].

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 system IS [3,4] so as to prevent, detect and respond to the threats which such systems are exposed to and therefore, protect information.

Á. Rocha et al. (eds.), *New Advances in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 445,
DOI 10.1007/978-3-319-31307-8_37

Information security is understood as the maintenance, assurance and compliance with the following features of information:

- Confidentiality: Information assets can only be accessed and handled by users who have permission for that.
- Integrity: The content of information assets must remain unaltered and complete. Any changes made must be recorded ensuring their reliability.
- Availability: Information assets can only be obtained in short term by users who have the appropriate permissions.

Information systems security (ISS) policies consist essentially of documents which guide or regulate the actions of people or systems within the ISS domain [5]. ISS policies are pointed out in literature as one of the main measures to be taken by organizations for protecting their IS.

Considering the fact that this work addresses SMEs, it is essential to define this latter concept. The status of SME is defined in the Decree-Law n. 272/2007 of November 6, according to the companies' number of permanent workers, which must be under 250; the turnover, which must be under or equal to 50 million Euros; and an annual balance-sheet total which must be under or equal to 43 million Euros.

In Table 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 table above, SMEs in Portugal represent 99.8% of business. Their representativeness is extremely high, which makes them deserve more attention in many respects.

The research question that guided this work was to what extent AR methodology is adequate to support the process leading to the adoption of ISS policies.

The aim was to conduct the whole process of applying an ISS policy in 10 SMEs by using the AR research method. Structurally, this paper is organized as follows. After this contextualization of the subject, in section 2, we analyze the process of applying a security policy. Consecutively, we present the main features of the AR research method. In section 4, we describe the efforts made to formulate, implement and adopt ISS policies in 10 SMEs, which is followed by a discussion. Finally, we enumerate the papers' main contribution, and suggestions for future work.

2 Deployment of a security 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).

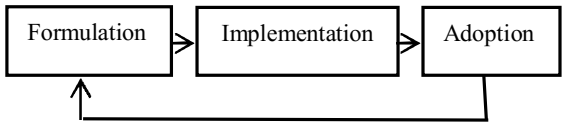

Fig. 1. The security policy application process.

The steps of this sequence, which starts with the formulation of the policy and ends with its adoption by the company, are consecutively described per se.

2.1 Formulation

In order to make IS secure, authors such as [6] claim that it is not always easy to write an IS policy 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 [7]. 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 [8].

According to [9], the development of a security policy within an organization involves four activities:

- Assessing and understanding the security needs;
- Reviewing the policies and procedures in use, if they happen to exist;
- Defining the protection requirements;
- Formalizing the security policy.

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 [10]. This process includes input elements which feed certain activity processes which, in turn, will originate a set of outputs.

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 [11].

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 IS • Identify required security controls • Compile security policy document • Write down security procedures • Compile the specifications for technical security controls	• Security policy for IS • Specification for countermeasures

Fig. 2. The process of security policy formulation.

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.

2.2 Implementation

The implementation of a policy is considered as a set of activities which aim to prescribe what is written in the policy document.

There are six main principles to be considered within the process of implementing an ISS policy [12]:

1. The organization will ensure that its information is kept safe and used in an appropriate way;
2. The organization will provide clear guidance to human resources regarding information security;
3. All human resources working for and on the behalf of the organization will cooperate with the information security policy within the organization;
4. The organization will ensure that its human resources know all the relevant guidelines regarding the organization's information security;
5. The organization will inform its clients about the way their records will be kept safe as well as of who will have access to them;
6. The organization will comply with all the national legislation as well as with the best guidance regarding information security.

The implementation of a policy is the process throughout which policies are turned into guidelines, procedures and lists of what to do and are put into practice by the information system users [10]. Thus, the implementation of an ISS policy can be considered as a set of activities aiming to prescribe what is written in the policy document.

In figure 3, we present a process of ISS policy implementation [10]. This process includes input elements which feed certain activity processes which, in turn, will originate a set of outputs.

Input	Activities	Output
• Security policy document • Knowledge on the culture of the organization	• Provide instructions on the application of the security policy • Provide the users of the IS with adequate training and education on the use of the security policy and procedures • Monitor and evaluate the use of the security policy • Monitor and evaluate security procedures • Implement technical and organizational security controls	• Security awareness • Evaluation of the implementation of use of the security policy and the application of security procedures

Fig. 3. The process of security policy implementation

This process ultimately results in the implementation and subsequent conscientiousness of both users and managers regarding the obligation of using the policy with utmost rigor and seriousness.

2.3 Adoption

Due to the nature of the diverse organizations where different and distinct users access and use the IS, the adoption and concomitant compliance with ISS policies is essential to enable the detection of flaws and incoherencies in the adoption process and to lead to their correction.

According to [10], the adoption of a policy includes elements of input, which feed certain procedures of activities, which in turn originate a set of outputs. figure 4 represents a scheme illustrating these authors' view.

Input	Activities	Output
• Evaluation of the use of the Security Policy • Established security procedures and work practices that implement the security policy • Education and training programs	• Establish norms that support security management • Promote the issue of security to IS users • Resolve possible conflicts and difficulties in the application of the security controls • Keep users and management informed on the IS security agenda	• Security culture • Proposals and requirements for improving and adjusting the security policy

Fig. 4. The process of security policy adoption

Within the process of adoption of an ISS policy, inputs include the evaluation of the policy during its implementation, the procedures and working practices which implement the security policy, and the users' training and education processes. Based on this information, the following process includes solving possible conflicts and difficulties detected in the application of certain parameters contained in the policy, and keeping users and managers informed on the ISS agenda.

3 Perspectives on Action Research

Both the description of the application of any research method and the lessons learnt from that application require a previous clarification. Such clarification goes from the way the different practitioners understand the research method to the method's main features and the way it is applied, as well as its areas of applicability.

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 [13]:

Action – the aim is to reach change within a community, organization or program;

Research – by increasing understanding by the practitioner, client or community.

Although different authors may have diverse perspectives concerning the usefulness of the AR method, there seem to be broad consensus regarding the method's general architecture. In short, the AR method starts with the detection of a problem, from which some changes are projected aiming to solve the problem. This process is cyclic as when applied to organizations or other social groups, it is unlikely that a problem is considered permanently solved and will rather suffer alterations and require new intervention. Thus, AR constitutes a methodological approach directed towards change: it is not limited to the understanding of phenomena but it also deliberately aims to change those phenomena.

The authors Susman and Evered [14] view a general AR project as a cyclical process, which is referred to by them as the AR cycle. According to their view, the typical AR cycle is composed of five stages: diagnosing; action planning; action taking; evaluating; and specifying learning. Diagnosing is concerned with the identification and definition of a problem to be solved in the client's organization. Action planning considers alternative courses of action to solve the problem. Action taking includes the selection and execution of one course of action. Evaluating comprises the study of the outcomes of the selected course of action. Specifying learning is the stage in which the study accomplished in the previous phases will be structured in the form of general findings.

As suggested in figure 5, the AR cycle takes place just after the Preparation phase. The Diagnosing involves a cooperative work between the researcher and the organization so that a problem to be solved during the research can be clearly identified. This identification has a more limited scope than that of the view expressed in the Preparation phase, and takes into consideration real implementation issues, e.g. the need for pilot projects and the availability of software systems. Following the Diagnosing are the Action Planning, Action Taking and Evaluating stages, all carried out in cooperation between the researcher and the client's organization. The next stage is Specifying Learning, typically carried out only by the researcher. This is the

stage in which the researcher will structure results so as to refine the set of open-ended questions, yet with appropriate answers to a number of them, and the preliminary model. Here, the researcher will decide if they will either proceed again in the cycle or go out to the Post-evaluation stage, summarized in the next section.

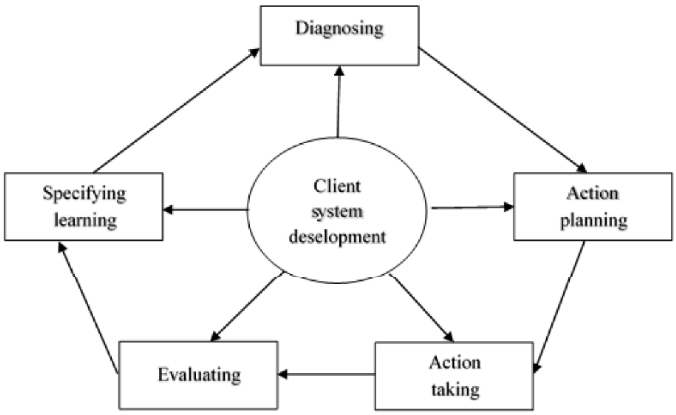

Fig. 5. Five steps AR cycle

Associated with each of the stages included in this model are the following goals:

- Diagnosing – Identification of a problematic situation, related to the need of change of a certain organization;
- Action Planning – Specification of the organizational actions which must be undertaken in order to solve the problems identified in the diagnostic;
- Action Taking – Implementation of the actions previously planned which will supposedly lead to changes;
- Evaluating – Assessment of the intended goals achievement and solution;
- Specifying Learning – Specification of the knowledge acquired with the introduced change.

4 Action Research applied to the security policy application process

This study involved ten SMEs through direct contact with the correspondent information technology departments and indirect contact with the direction as well as the users of the IS. This work reports on the use and appropriateness of AR applied to the formulation, implementation and adoption of ISS policies, thus contributing as an empirical study on the application of that method in the field of IS.

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: The SMEs geographic location; Their dimension; The fact that they did not have an

implemented ISS policy and 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 spent 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.

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 information technology department (8 cases) and with the owner of the company (2 cases).

After these steps, the policy document was finalized jointly with the stakeholders mentioned above and we proceeded to its implementation. As far as the adoption of the policies by the companies is concerned, this step was taken 8 months after implementation. This time lag was owed to the fact that not all the policies which are implemented are consecutively adopted. They often fade to oblivion, what is defined in the document is not followed by the information system users, the policies are never reviewed or updated.

In the first stage – Diagnosing – a problematic situation was identified, namely the non adoption of an ISS policy in SMEs. In other words, although the problem was recognized and assumed, the organizations had not been able to create the conditions to change the situation. Such acknowledgement reinforced the conviction that the AR method might prove to be particularly appropriate to change the current practice.

In the second stage of AR – Action Planning – the organizational actions which must be undertaken in order to solve the problems identified in the diagnostic are specified. In the present study, this process started with the drafting of the ISS policy document. We planned to draft the policy following a model proposed by the researcher, but adapted to the reality of each SME in a joint work with the elements from the information technology department.

In the third stage of the AR cycle, called – Action Taking – the planned actions are implemented in the hope that they will lead to some change in the organization. In our study, this stage involved several steps, namely the implementation of the policy; its approval; and its further dissemination.

The fourth stage – Evaluating – assesses whether the goals intended with the implementation of the ISS policy were achieved or not. Such evaluation involves the review of the policy, which must take place on a regular basis and particularly whenever significant changes occur within the company, in order to ensure that the policy continues to fulfill the purposes for which it was implemented. In this study, evaluation was carried out by checking users' compliance with the policy. A review of the policies was not considered necessary at this point.

The last stage – Specifying Learning – takes place in the end, as a conclusion of the whole process. However, this stage is actually present throughout the whole AR cycle. In this study, learning throughout the cycle provided a starting point for a new planning, thus, setting the beginning of a new sequence of the cycle.

The various phases of AR which were explained above are now summarized in Table 2, in which we present the five stages of Susman and Evered (figure 5) model as well as the main facts developed during each of them.

Table 2. AR stages in the implementation of an ISS policy

Diagnosing	Action Planning	Action Taking	Evaluating	Specifying Learning
-Lack of an ISS policy -Lack of initiative -Lack of an ISS policy model -Importance of a policy -Defining a problem	-Providing an ISS policy model -Drafting an ISS policy document -Planning the policy implementation -Defining ways to approve and disseminate the policy	-Implementing what was defined in the last stage	-Checking compliance with the policy -Checking the policy updating	-Assessing -Stopping if the problem is solved or if not, starting a second cycle.

5 Discussion

With this work, 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. 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.

This research method allows the participants to obtain a very wide knowledge of the company, which enables the formulation, implementation and adoption of a policy which can fit perfectly into the reality of each SME.

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.

6 Conclusion

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, implementation and adoption of ISS policies in SMEs.

Among the works which might be carried out in the future, we highlight the proposal of an ISS policy model, thought up for the national reality, and which may work as a starting point to the adoption of ISS policies by SMEs, so as to invert the reduced number of policies existent in the SMEs. The provision of that document by SMEs and the use of AR as a method for planning and promoting change, in which researchers and practitioners project actions, implement them, and evaluate their impacts, may prove to be two important tools for the institutionalization of ISS policies in organizations.

Acknowledgment

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

References

1. Lopes, I. and Oliveira, P.: Understanding Information Security Culture: A Survey in SMEs. Álvaro Rocha, et al. A Stroetmann. New Perspectives in Information Systems and Technologies, Volume 1. ed. Cham: Springer, 2014, v. 275, pp. 277-286 (2014)
2. Da Veiga, A., Eloff, J. H. P.: An Information Security Governance Framework, Information Systems Management, 24:4, pp. 361-372 (2007)
3. Kim, D., Solomon, M. G.: Fundamentals of Information Systems Security, Jones and Bartlett Publishers (2010)
4. Tipton, H., Krause, M.: Information Security Mangement Handbook. Auerbach Publications (2009)
5. de Sá-Soares, F.: A Theory of Action Interpretation of Information Systems Security, PhD Thesis, University of Minho, Guimarães (2005)
6. Höne, K., Eloff, J.: Information security policy — what do international information security standards say?, Computers & Security 21 (5), pp. 402–409 (2012)
7. Wood, C. C.: Writing InfoSec Policies, Computers & Security, 14 (8), pp. 667-674 (1995)
8. Peltier, T. R.: ISS, Procedure: a practitioner's reference, CRC Press (1999)
9. Hartley, B., Locke, A.: The Process of Security, Business Security Advisor, pp. 22-24, USA (2001)
10. Karyda, M., Kiountouzis, E., Kokolakis, S.: Information systems security policies: a contextual perspective, Computers & Security 24 (3) pp. 246-260 (2005)
11. Wills, L.: Security Policies: Where to Begin, Security Essentials, 1(4b) (2002)
12. Gaunt, N.: Installing an appropriate information security policy, International Journal of Medical Informatics 49(1) pp. 131-134 (1998)
13. Dick, B.: A beginner's guide to action research (2000), (Accessed 4 de Dez 2014) www.scu.edu.au/schools/gcm/ar/arp/guide.html
14. Susman, G., Evered, R.: An Assessment of the Scientific Merits of Action Research, Administrative Science Quarterly, 23(4), pp 582-603 (1978)