Evaluation of the Adoption of an Information Systems Security Policy

Isabel Maria Lopes
Polytechnic Institute of Bragança
School of Technology and Management
Bragança, Portugal
isalopes@ipb.pt

Pedro Oliveira
Polytechnic Institute of Bragança
School of Technology and Management
Bragança, Portugal
pedrooli@ipb.pt

Abstract — **Information Systems Security (ISS) is a relevant fact for current 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 in particular, and information security in general. 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. A recent survey concluded that among 307 SMEs, only 15 indicated to have an ISS policy. 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, an academic-practitioner collaboration effort was established regarding the implementation of ISS policies in three SMEs. These interventions were conceived as Action Research (AR) projects.**

This article aims to constitute an empirical study on the applicability of the Action Research method in information systems, more specifically by assessing the adoption of an ISS policy in six SMEs, and identifying the critical success factors in adopting an ISS policy. The research question we intend to answer 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 evaluation of ISS policies adoption. It can both act as a research method that improves the understanding about the reasons why the policy has been abandoned, for example by the users, and as a change method, assisting practitioners to overcome barriers and suggesting measures to be implemented in order to allow the ISS policy to be properly followed by all the company users on a daily basis.

Keywords - Action Research; Information Systems Security; Small and Medium Sized Enterprises.

I. ADOPTION OF INFORMATION SYSTEMS SECURITY POLICIES

The increasing dependence of organizations in general and SMEs in particular on their information systems has led to a higher value of information, which has assumed a vital relevance to organizations. In the past, the main focus of organizations lied essentially on their tangible assets (physical and financial). However, over the last years, this reality has been altered and nowadays, organizations have included in their main focus another asset – information.

Information systems security is a critical issue to be taken into account within organizations worldwide, regardless of their size or location. Due to the growing number of threats to which information is submitted, the need to protect information systems reveals to be increasingly more pertinent and imperative.

There are several measures which can and must be implemented within SMEs in order to ensure the effective functioning of ISS. According to Höne and Eloff [1], "these measures include technical solutions and contractual regulations as well as organizational warnings regarding common risks, threats and vulnerabilities. Undoubtedly, the most important singularity of these provisions is the information security policy."

Nowadays, the adoption of measures such as the implementation of an ISS policy which may contribute for preserving information confidentiality, integrity and availability represents a demand within any organization. These are "documents which guide or regulate people or systems' actions in the domain of information systems security" [2]. Another author, Gilbert [3], defines policy as "the rules and procedures chosen to dictate future actions."

The importance of ISS Policies is stressed by several authors, such as Peltier [4], who classifies them as the "cornerstone of an effective information security architecture". According to Kee [5], security policies are "the Foundation and the base line of information security within an organization."

In order to implement 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 of formulation – implementation – revision – adoption of the policy.

When focusing our attention on a specific type of organization – SMEs – a study carried out by [6] 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 and ISS policy has not become a reality in SMEs yet.

This paper aims to constitute an empirical study on the applicability of the AR method in the field of Information, more specifically analyzing the adoption of ISS policies in SMEs and identifying the critical success factors in adopting an ISS policy. Hence, 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.

Structurally, this paper is organized as follows. After this contextualization of the topic under study, we briefly present what is understood by the adoption of an ISS policy, and we review the main tenets and characteristics of AR in general. Thereafter, we describe the way in which the AR steps were applied towards the adoption of an ISS policy by the companies. The discussion of results presents a set of critical success points that ensure a successful adoption of an ISS policy. Finally, we enumerate the papers' main contribution, limitations, and suggestions for future works.

II. Perspectives and Characterization of the Action Research

Given the aim proposed for this study as well as the philosophical framework guiding the researchers, the research method chosen for the present study was "Action Research". Hereafter, we briefly define this research method as well as its characteristics and applicability within the field of ISS policies.

AR considers the iterative process of interaction and focus on a research problem. Therefore, the first step to trigger it is identifying the problem and formulating it into a goal and in a way that it can be operated. The intervention aspect of AR means that it is an especially interesting and relevant method for the area of information systems development [7].

AR can be described as a family of research methodologies which pursue action (or change) and research (or understanding) at the same time. It is characterized by the cyclic revision of action followed by reflection, often culminating in the refinement of understanding using methods such as modelling. The iterative nature of the methodology promotes convergence to a greater understanding [8].

Williams [9] described AR as similar to the case study approach in describing the richness of an environment, and as similar to field experimentation in working in situ, but adding to these features intervention and reflection. The strengths of the AR method lie on its iterative cycle within a real-world context of assessment, action and reflection, with potential participant input and practical and applicable outcomes.

According to [10], AR is essentially an in loco procedure which views to tackle a concrete problem located within an immediate situation. The process is controlled step by step during varying periods of time, through diverse data collection techniques (questionnaire, interviews, etc.) and the subsequent results must enable the introduction of changes, adjustments, direction changes and redefinitions according to needs, which may bring long-lasting advantages to the on-course process itself.

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.

What best characterizes and identifies AR is the fact that it is a research methodology essentially practical and applied which is ruled by the need to solve real problems. Along with the research, there is an action which aims to transform reality and subsequently, produce knowledge of the transformations resulting from the action [11].

AR is ruled by the need to solve real problems and assumes some essential characteristics pointed out by authors such as Dick [12], Descombe [13], and Cohen and Manion [10]:

- Participatory and collaborative – as all the participants are involved in the process. They all are co-actors of the research. The practitioner is not an external agent who does research with people, but a co-researcher with and for those who are interested in practical problems and in improving situations.
- Practical and interventional – it is not limited to the theoretical field of describing a certain reality. Action must be linked to change and is always deliberate.
- Cyclic – The research involves a spiral of cycles in which the initial findings generate possibilities of change, which are implemented and assessed as an introduction to the following cycle. The cycle varies according to the author, but it includes at least the following stages: Planning – Action – Reflection.
- Critical – The critical community of participants are not only looking for better practices concerning their work, within certain sociopolitical restrictions, but they also act as agents of change, critics and self-critics regarding possible restrictions. They change their environment and are transformed in the process.
- Self-assessing – Changes are continuously assessed within a perspective of adaptability and production of new knowledge.
- Qualitative – it is predominantly qualitative although some situations may require some quantification.

According to Pring [14], some of the key features of Action Research are:

- Cyclic and recursive. Similar situations tend to repeat themselves in similar ways.
- Participatory. The participants in the research process have bonds of cooption, cooperation and collaboration.
- Qualitative. It deals more with ideas than with figures.

- Reflexive. Critical reflection on the process and its results is an important stage of each cycle.

AR is characterized by a set of stages whose sequence enables the implementation of the method within a certain context and the solving of a certain problem. Different authors present different stages. Among such a wide variety of models, we selected four, as we consider this number to be sufficient to illustrate their scope and differences.

Cunha and Figueiredo [15] present a model adapted from Dick (1992) which includes three steps: Planning; Action; and Reflection, as presented in Fig. 1.

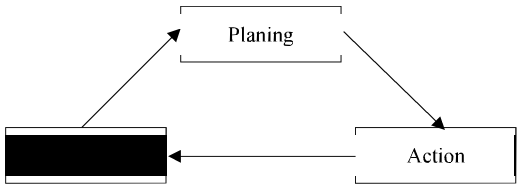

Figure 1. Three steps AR cycle

Based on these three building blocks, [15] 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)."

According to [16] and [17], the AR cyclic process or spiral comprises four different stages, namely planning; action; observation; and reflection. For this author, it is normal for an AR project to go through two or more iterative cycles. The product resulting from each cycle improves as the cycles are repeated, and each of these cycles includes reflections on the previous ones.

Cohen and Manion [10] view the development of an AR project through the following steps:

- Identification, assessment and formulation of a problem;
- Preliminary discussion and negotiation between the parties involved;
- Review of literature regarding the field of research;
- Review of the initial problem formulation;
- Selection of research procedures;
- Selection of assessment procedures;
- Implementation of the project;
- Interpretation of the collected data.

Susman and Evered [18] view a general AR project as a cyclic 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 related to 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 a 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 (cf. Fig. 2).

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 within 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. Although this stage appears as the last one in the scheme, it represents a permanent process.

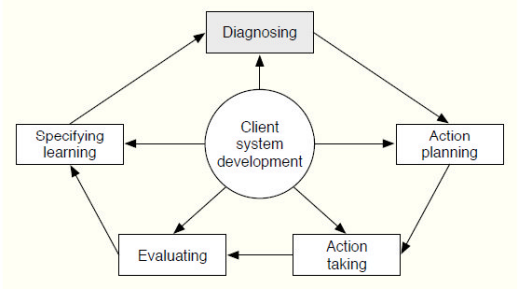

Figure 2. Five steps AR cycle

III. Action Research Applied to the Adoption of Information Systems Security Policies

Action Research was primarily applied in the academic milieus of Social and Medical Sciences, but in 1990, it started to be successfully explored in the areas of Educational Sciences, organizations learning and Information Systems [19].

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 [20].

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." [21].

For these reasons, we consider that the application of the AR research method is adequate to study the adoption of ISS policies by SMEs.

The creation of an ISS policy follows a complete life cycle from its formulation to its adoption, including its implementation and review. This study mainly focuses on the stage of adoption of an ISS policy. Therefore, before presenting the results of the study, we will briefly present what is understood by the adoption of an ISS policy.

Due to the nature of the diverse organizations where different and distinct users access and use the information system, 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 Karyda [22], the adoption of a policy includes elements of input, which feed certain procedures of activities, which in turn originate a set of outputs. Fig. 3, 4 and 5 represents a scheme illustrating these authors' view.

Input

- Evaluation of the use of the Security Policy
- Established security procedures and work practices that implement the security policy
- Education and training programs

Figure 3. The process of security policy adoption (Input)

Activities

- 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

Figure 4. The process of security policy adoption (Activities)

Output

- Security culture
- Proposals and requirements for improving and adjusting the security policy

Figure 5. The process of security policy adoption (Output)

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 keep users and managers informed on the ISS agenda.

This process of adoption of a policy is coincident with the AR cyclic model mentioned in point 3 of this study in many respects. Therefore, this study was structured according to the model proposed by [18], which is composed of five steps: Diagnosing; Action planning; Action taking; Evaluation and Specifying learning (cf. Fig. 2).

As it has been mentioned above, the AR cycle starts with the detection of a problem. In this study, identifying the problem was a simple and unambiguous task. Such detection derived from acknowledging the study carried out by [6], in which 307 SMEs heads of the IT department were inquired about the existence or not of an ISS policy in their company, and in which the results showed that only 15 of the companies stated to have an ISS policy in their organization.

Having identified the problem, the present study aimed to verify whether or not the ISS policy implemented in the organizations is truly adopted by them. In other words, the aim of this study is to detect the critical success factors in the adoption an ISS policy. In order to achieve this aim, we studied six SMEs and assessed in loco whether or not the ISS policies are respected and followed by users in the organization's day-to-day activity and what critical success factors impact on their adoption. The time spend in each SME was approximately one week, with periodic sectorial meetings.

In the first stage – Diagnosing – a problematic situation was identified, namely the non-institutionalization of an ISS policy by SMEs. Companies recognize the importance of a policy for the security of their assets, namely information. However, few are able to implement one and therefore, originate a context of change within the organization. Nevertheless, the main question to be answered is to what extent the policies which were implemented by the companies were actually adopted by those companies. On these grounds, conviction was reinforced that AR may reveal particularly adequate to change this situation.

The researcher was faced with the realities of the six SMEs, making a first contact with the company through the Head of the IT department, questioning them about whether or not the ISS policy previously implemented was being adopted. It was found that although all the interviewees wanted the policy to be adopted within the organization, such adoption was not taking place in 4 of the companies.

In two cases, the reason pointed out for the non-adoption was the users' lack of awareness towards the information security issue, thus not respecting the provisions established in the policy. In one case, the policy document revealed to be very long and confusing, which made its implementation difficult. In another company, the Head of the IT department took responsibility for the non-adoption of the policy, stating that he had failed to disseminate the policy among all users and had not taken the necessary actions for its implementation.

In the second stage – Action Planning – we specified the actions which had to be executed so that the ISS policy could be implemented. Those actions were formulated jointly by the researcher and the company's representative accompanying the

process. The process started with a review of the document in the four SMEs. In three of them, some adjustments were made, and in one of the cases, the document was almost completely redrawn. After this, and before moving on to the implementation planning, we analyzed the factors which had previously failed so that similar mistakes would not be repeated.

Besides planning the actions to be executed in order to implement the policy itself, the Heads of the IT department in the six companies and the researcher jointly contributed with their experience to draw a set of critical success points to the adoption of the ISS policy.

In the third stage – Action – we implemented the actions previously defined, expecting that these would lead to a change within the organization. This step involved several phases, starting with the review of the policy document, moving on to its approval by the executive board and further on to its dissemination among all users.

The fourth stage, called – Evaluation – aims to assess whether or not the goals were achieved and the problems were solved. This evaluation requires the review of the ISS policy, which must take place within a well-defined time frame, or whenever significant changes are observed within the company for the policy to continue to play its role. In the six companies involved in this study, evaluation was carried out by checking users' compliance with the provisions established in the policy. As far as the review of the policy is concerned, we considered that it was not necessary yet.

The last stage – Learning – is usually listed at the end of the process. However, it is a permanent process since the learning occurring throughout the whole cycle can be used as a starting point for a new cycle whenever necessary.

IV. Discussion

AR is an emergent methodology as it provides flexibility, adequate answers and change. Its process is well adjusted to the demands of the situation in all its complexity. AR open attitude towards knowledge enables this method to provide a more effective change, which in turn, stimulates a more effective understanding of the problem.

By using this methodology, we tried to help SMEs change a concrete situation, which was the non-adoption of an ISS policy. Also, we tried to understand that specific situation and to alter it. The goal concerning the adoption of an ISS policy by the four SMEs was achieved by identifying and later on implementing the key-points to its adoption, or in other words, the factors considered as critical to the success of a policy.

We hereafter present a brief list of critical success factors to the adoption of an ISS policy, identifying the aspects pointed out as crucial by the members in charge for the six SMEs involved in this study.

The success of a policy highly depends on the adoption and compliance with the policy by its users. It is important to draw individual responsibilities, for instance, by clarifying who has access to each specific part of the system.

Another aspect which was considered as a critical success factor to a good implementation is the definition of sanctions for users who do not comply with the provisions of the policy.

Having the support of the organizations' managers in the formulation and adoption of the policies is also an essential critical factor to the success of an ISS policy. Only the involvement of all cooperators and mainly the involvement of managers and executives can grant a good formulation and adoption of the policy.

The periodic review of ISS policies is also crucial. A policy by itself will be of little use if it is not updated. Organizations are increasingly more dynamic and as a consequence, changes in structure or in the way they operate happen at a highly quick pace. Therefore, it is necessary to adapt the policy to those new realities.

The communication and dissemination of the policy among all those who must know it and comply with it have also been pointed out as being crucial to the success of the policies. It is easily understood that all users must acknowledge the existence of a security policy as well as its contents. Although the ways to disseminate the policy document may vary (internal memorandum, provision of the policy on the organization's intranet, or other mechanisms), it is necessary to ensure everybody's acknowledgment of the policy content.

Integrating the policy with the organization's goals, processes and culture is fundamental for the success of its implementation. An ISS policy must be a constructive and protective vehicle and never a mechanism which may hinder the good development of the organization's functioning. In order to achieve this, it is necessary that the creators of the policy take into account the company's goals as well as its organizational processes and culture before drawing the document.

The policies workability (regarding their implementation and compliance) represents another essential factor. Having an ISS policy will be by itself of little use if its workability reveals to be impossible.

It is necessary to raise awareness of the people involved towards the fact that technology is not the only element to take into account. Without an ISS policy, but also without methods of response to incidents or a business continuity plan, technologies will not be effective in the protection of the organization's information.

One more aspect to consider is related to both users and managers' awareness towards security issues. This aspect is particularly relevant as the human factor is pointed out as the main responsible for the majority of incidents regarding security. Therefore, awareness towards such issues is fundamental to enable the organizational ISS policy to produce the desired result [23].

The ISS policy must include a set of guidelines, provisions and procedures which must be obeyed with a view to raising users' awareness and guiding them towards a secure use of technologies. Therefore, the policy must contain information on how to manage, save and protect one of the company's main assets – information.

V. CONCLUSION

The process of adopting an ISS policy involves a set of stages which include inputs and effective activities. The process developed in this study can also be considered as the effective process of the policy since the evaluation process started simultaneously with its implementation, resulting in a real awareness raising concerning the importance of the policy and the subsequent organizational culture as well as in feedback for possible adjustments of the policy.

It was possible to conduct these stages, which involve a dynamic of action – reflection – action, by using the AR methodology, which proved to be effective to the adoption of an ISS policy in the four SMEs taking part in the study. This research work involved six SMEs, two of which had already adopted a policy, thus enabling the collection of distinct data, namely the key-points to a well-succeeded adoption. In the remaining four SMEs, the work which was carried out required a bigger proximity in order to rectify the problem identified, which consisted of the non-adoption of the ISS policy in the day-to-day operations of the organization.

This research work presents limitations, namely with respect to the number of SMEs involved. Although we believe that the study carried out in the six 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.

Throughout this study, some guidelines were identified regarding the development of future works. Consequently, we found two promising starting points for further studies. The first point consists of a proposal of an ISS policy model that can be followed by SMEs in order to facilitate their formulation and further implementation of a policy on their own. The second point is based on the premise that the issue of information security is common to different organisms. Therefore, comparing different policies from diverse organizations may represent a good proposal of research.

REFERENCES

[1] K. Höne, e J. Eloff, "Information security policy — what do international information security standards say?", Computers & Security 21 (5), pp. 402–409, 2002.

[2] F. de Sá-Soares, A Theory of Action Interpretation of IS Security, PhD Thesis, University of Minho, Guimarães, 2005.

[3] C. Gilbert, "Guidelines for an Information Sharing Policy", SANS Institute, 2003.

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

[5] C. Kee, "Security Policy Roadmap – Process for Creating Security Policies", SANS Institute, 2001.

[6] I. Lopes, and P. Oliveira, "Understanding Information Security Culture: A Survey in SMEs Enterprises", Álvaro Rocha, Ana Maria Correia, Felix . B TanKarl. A Stroetmann. New Perspectives in Information Systems and Technologies, Volume 1. ed. Cham: Springer International Publishing, 2014, vol. 275, pp. 277-286, 2014.

[7] D. E. Avison, A. T. Wood-Harper, R. T. Vidgen, and J. R. G. Wood, A further exploration into IS development: the evolution of Multiview 2. Information, Technology and People, 11 (2), pp. 124–139, 1998.

[8] B. Dick, "What is action research?" 1999. (Accessed 30-06-2013) www.scu.edu.au/schools/gcm/ar/whatisar.html.

[9] P. Williams, "Making Research Real: Information Systems Action Research a Suitable Methodology for Medical IS Security Investigations?", Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Western Australia, 2006.

[10] L. Cohen and L. Manion, "Research Methods in Education", London, Routledge, 1994.

[11] M. Hugon and C. Seibel, Recherches impliquées. Recherche action: le cas de l'éducation – Bruxelles: De Boock Wesmael, 1988.

[12] B. Dick, "A beginner's guide to action research", 2000. (Acessed em 4-12-2006). www.scu.edu.au/schools/gcm/ar/arp/guide.html.

[13] M. Descombe, "The Good Research Guide for Small-Scale Social Research", Buckingham: Open University Press, 1999.

[14] R. Pring, "The "False dualism" of educational research", Journal of Philosophy of Education, 34 (2), pp. 247-260, 2000.

[15] P. R. Cunha, and A. D. Figueiredo, "Action Research and Critical Rationalism: a Virtuous Marriage", Proceedings of the 10th European Conference on Information Systems, Gdansk, Poland, 2002,

[16] D. Kember, "Action Learning and Action Research: Improving the quality of Teaching & Learning", USA:Stylus Publishing Inc, 2000.

[17] Zuber-Skerritt, "Action Research in Higher Education: Examples and Reflections", Kogan Page, London, 1996.

[18] G. Susman, and R. Evered, "An Assessment of the Scientific Merits of Action Research, Administrative Science Quarterly", 23(4), pp. 582-603, 1978.

[19] R. Baskerville, "Investigating Information System With Action Research", CAIS, 2(19), pp. 1-32, 1999.

[20] F. Silva, "A Investigação Qualitativa na Avaliação de SI para a Gestão Empresarial, Workshop em Investigação Qualitativa", 3ª CAPSI, Coimbra, 2002.

[21] R. Baskerville and A. T. Wood-Harper, "A Critical Perspective on Action Research as Method for IS Research", Journal of Information Technology, 3(11), pp 235-246, 1996.

[22] M. Karyda, E. Kiountouzis, and S. Kokolakis, "Information Systems security policies: a contextual perspective", Computers & Security 24 (3) pp. 246-260, 2005.

[23] I. Lopes, "The adoption of information security systems in the local public administration in Portugal", PhD Thesis, University of Minho, Guimarães, 2012.