Structure and Challenges of a Security Policy on Small and Medium Enterprises

Fernando Almeida[1], Inês Carvalho[2] and Fábio Cruz[2]
[1] Faculty of Engineering of Oporto University, INESC TEC & ISPGaya
Porto, PT 4200-464 - Portugal
[e-mail: almd@fe.up.pt]
[2] School of Computer Science and Engineering, Higher Institute of Gaya, ISPGaya
Vila Nova de Gaia, VNG 4400-103 - Portugal
[e-mail: ispg3956@ispgaya.pt, ispg3932@ispgaya.pt]
*Corresponding author: Fernando Almeida

Received May 29, 2017; revised August 28, 2017; accepted September 8, 2017; published February 28, 2018

Abstract

Information Technology (IT) plays an increasingly important role for small and medium-sized enterprises. It has become fundamental for these companies to protect information and IT assets in relation to risks and threats that have grown in recent years. This study aims to understand the importance and structure of an information security policy, using a quantitative study that intends to identify the most important and least relevant elements of an information security policy document. The findings of this study reveal that the top three most important elements in the structure of a security policy are the asset management, security risk management and define the scope of the policy. On the other side, the three least relevant elements include the executive summary, contacts and manual inspection. Additionally, the study reveals that the importance given to each element of the security policy is slightly changed according to the sectors of activity. The elements that show the greatest variability are the review process, executive summary and penalties. On the other side, the purpose of the policy and the asset management present a stable importance for all sectors of activity.

Keywords: security policy, SMEs, privacy, information assets, risk management

1. Introduction

The field of Information Systems Management is clearly one of the main challenges facing companies today, driven by the pressure to reach higher levels of individual and collective productivity, with the consequent need of optimizing existing processes and necessary structural changes.

In this sense, the increasing dependence on information technology (IT) in the business environment, coupled with the increasing reliance of information systems in organizations, makes the management of information security an important tool in corporate management. Thus, companies must necessarily understand that information security is today a business problem, not just technology.

Small and medium-sized enterprises (SMEs) generally do not care about information security because they believe that are not important enough to target criminals and, therefore, do not see value investing in this area. In fact, there is a lack of understanding about how security is important to the business and what are the consequences of a successful attack. If large companies lose millions in major attacks, for small businesses the damage can be catastrophic. According to the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), the number of valid cybercrime complaints received in 2012 was 24,000 per month and the amount of losses related to cybercrime increased by 8.3% since 2011 [1]. More recently, the Federation of Small Businesses (FSB) has also confirmed this issue by alerting that these attacks cost around £5.26 billion to the UK economy [2].

The information has emerged as the most valuable asset of organizations, and can be the target of a series of threats in order to exploit the vulnerabilities and cause considerable damage for SMEs [3-4]. Therefore, it is necessary to implement information security policies that seek to reduce the chances of fraud or loss of information.

The Information Security Policy (ISP) is a document that should contain a set of standards, methods and procedures, which should be communicated to all employees as well as critically reviewed and reviewed at regular intervals or when changes are needed. In order to prepare an ISP, consideration should be given to ISO 27001:2013 (belongs to the ISO/IEC 27000 family of standards), which is a standard of codes of practice for information security management. This document offers a package of best practices that may be used to initiate, implement, maintain and improve the management of information security in an organization.

This paper investigates the role of information security policies on SMEs. The idea is to analyze the structure of an information security policy and understand its most important and least important elements in the perspective of those companies. It is the first study in the field that makes a comparative analyzes about the relative importance of those elements and analyzes their relevance according to the sector of activity of the SMEs. The paper is structured as follows: we initially perform a revision of literature in the field by identifying the most predominant studies. After that initial phase, we present the structure of the adopted methodology. Then, the results of the study are listed and discussed. Finally, the conclusions of this work are drawn.

2. Related Work

In this section, we consider some related works in the field of information security principles and risks in SMEs. Additionally, we also look at the approaches and challenges of the establishment of an information security policy faced by them.

Nowadays it is crucial for every company or institution to have and use mechanisms for storing and securing their information. Information security is guaranteed using effective and up-to-date security mechanisms. In the most diverse areas of information technology, we find security approaches and protocols for mobile, ad hoc and IoT networks [5-7].

The European Union Agency for Network and Information Security (ENISA) develops advices and recommendations for good practice in information security among the EU Member States. The study conducted by Manso et al. [8] showed that, despite rising concerns about information security risks, the level of SMEs information security and privacy standard adoption is relatively low. The main identified barriers are: (i) barriers related to knowledge and engagement; (ii) barriers related to available capabilities and resources; (iii) barriers related to shortage of standards in specific areas; and (iv) barriers related to implementation aspects. Additionally, the study proposes the following key recommendations to improve the information security and privacy standardization level in the European SME community: (i) increasing knowledge and engagement; (ii) driving adoption and compliance; (iii) facilitating implementation; (iv) increasing capabilities; and (v) fostering cooperation.

In addition to information security, there are also several studies that look and propose support decision models specifically addressed to the SME sector [9-10]. In this sense, it becomes clear that the SME sector is gaining increasing importance in information technologies, both in industry and services environment.

Lacey and James [11] develop a research project where they identify and evaluate the needs of small and medium sized organizations (SMEs) for advice on information security, particularly concerning the shielding of personal information, and how these requirements are as of now being met, or could be better met, by public sources of security guidance.

Tawileh et al. [12] identify the main challenges impeding the implementation of information security management in SMEs and propose a holistic approach based on Soft System Methodology to encourage and facilitate the development of security management systems within SMEs.

Soomro et al. [13] advise that information security management needs a more holistic approach. The authors give a comprehensive picture of such approach and performs a systematic literature review approach that synthesize literature related to management roles in information security to explore specific managerial activities to enhance information security management.

The study [14] exposes that SMEs lacks to have an appropriate security IT infrastructure due to financial restrictions, limited resources, and adequate know-how. Additionally, it confirms the importance of a holistic approach and proposes the existence of four levels: (i) organizational; (ii) workflow; (iii) information; and (iv) technical.

In the research [15], the authors have developed semi-structured interviews with 19 managers of SMEs in order to realize their views about security issues, such as confidentiality, integrity, availability and non-repudiations. The study found that they consider security information as an important asset, but most are only reactive in administrating information security, which results in financial losses and reputation.

The study conducted by Kluitenberg [16] looks to the predominance of defense measures, policies and their use in SMEs. The study adopts a quantitative technique based on questionnaires and looks only in the IT service industry. The results point out issues in the following areas: (i) web authentication; (ii) cloud for file-exchange; (iii) use of pirated software; (iv) and lack of enforcement of installation policies.

Amrin [17] confirms that SMEs lacks a decent level point of IT security. Some SMEs lack to have a written security policy and most of them don't implement IT security measures and policy. Furthermore, Bring Your Own Device (BYOD) and Cloud Computing are two emergent vulnerabilities.

Renaud [18] states that security vulnerabilities are currently more visible in SMEs rather than in big companies since they are perceived to have the weakest defenses. Additionally, she advocates that there is compelling evidence that SMEs are not taking the necessary steps to protect themselves.

Santos-Olmo et al. [19] highlight the importance of the security culture in SMEs. Furthermore, they describe how the concept of security culture has been introduced into the "Information Security Management System in SMEs" (MARISMA) developed by the Sicaman Nuevas Tecnologías Company, Research Group GSyA and Alarcos of the University of Castilla-La Mancha.

The work done by Alshaikh et al. [20] provide an ample overview of the management practices of information security policy and builds up a practice-based model, which can be used by practitioners to benchmark their current security practices.

The study conducted by Peltier [21] is another relevant reference in the field of implementing a security policy. It looks for elements that should be included in an information security program. It emphasizes the role of organization personnel, the segmentation of the audience and the effectiveness of content.

Lopes and Oliveira [22] give also important contributions in this field by the development of two pertinent studies in this field. The first study [22] characterizes the critical success factors for the implementation of a security policy in the context of SMEs. The second study [23] analyzes the implementation of security policies in 25 City Councils in terms of features and components.

Sadok and Bednar [24] performed a study among 33 SMEs in the UK about how they approach information security risks and what the human and organizational issues related to their risk-management practices are. The findings of this study let us to conclude that there is a wide agreement on the importance of security and its potential impact on company performance.

Alqatawna [25] looks to the main challenges of implementing information security standards in SMEs. The paper analyzes the three major security standards (Common Criteria, System Security Engineering-Capability and Maturity Model and ISO/IEC 27001) and exposes the main difficulties of implementing them in SMEs.

Cholez and Girard [26] present a study about the maturity assessment and process improvement for information security management in SMEs. The research proposes a method adapted to SMEs to conduct a first assessment of the enterprise information security maturity and improve their process accordingly.

Finally, Mijnhardt et al. [27] look at the organizational characteristics that are influencing SMEs in the adoption and use of information security maturity models. The study uses the Information Security Focus Area Maturity (ISFAM) framework for SME information security

and proposes a new model entitled CHOISS (Characterizing Organizations' Information Security for SMEs), which categorizes organizational characteristics in four categories through 47 parameters to help SMEs distinguish and prioritize which risks to mitigate.

Finally, **Table 1** presents a comparative analysis of the main security risks and barriers among the most recent studies (published since 2016). Studies are distributed on the table according to their appearance in the manuscript. There, rows correspond to security risks and barrier identified in these studies. Acronyms used to represent the different alternatives were the following: "Y-yes", "N-no", and "P-partial," It is possible to conclude that the studies can be typically divided into two categories: (i) technical orientation studies that essentially look to the technical vulnerabilities of equipments, protocols and policies; and (ii) management orientation that essentially look at security vulnerabilities from a social perspective, where top managers and employees play a central role.

Table 1. Comparative analysis of main recent studies on security risks and barriers

Security risks and barriers	Ref5	Ref6	Ref13	Ref18	Ref19	Ref24	Ref27
Eavesdropping	Y	Y	N	N	P	P	N
Flooding attack	Y	N	N	N	P	P	N
Denial of service	Y	N	N	N	P	P	N
Malware	N	N	N	Y	P	P	N
Top management support	N	N	Y	P	Y	Y	Y
Employee's behavior	N	N	Y	P	Y	Y	Y
Access policy violation	N	N	Y	Y	P	P	P
Bad secure configuration	N	N	P	Y	N	N	P

3. Methodology

This study aims to analyze the structure of an information security policy for SMEs. In order to reach this purpose and gather this data, the study adopts a quantitative approach based on a questionnaire created using the Google Drive platform and delivered it through two professional LinkedIn groups in IT security field. The questionnaire was available between 13th of February 2017 and 17th of March 2017.

The quantitative approach adopted brings us two important benefits: (i) provides results which can be condensed to statistics (e.g., mean, standard deviation, quartiles, hypothesis testing; and (ii) allows for statistical comparison between various groups. Additionally, we adopted the evaluation criteria for quantitative research proposal to ensure that the characteristics of this study justify the use of a quantitative methodology [28].

The questionnaire is composed of 46 questions divided into six sections. These sections were defined attending the ISO/IEC 27001, ISFAM and CHOISS in order to guarantee a low capital expenditures (CAPEX) and operating expenses (OPEX). The structure of the security policy presents a high vertical (e.g., changing the number of sections) and horizontal scalability (e.g., changing the number of variables), which is a fundamental element for its adoption by SMEs. The purpose of each section is mentioned in **Table 2**.

Table 2. Structure of the questionnaire

Section	Description
Control data	Information regarding the dimension, industry and the role of the respondent.
Contextualization	Elements that must appear on the cover and/or on the preamble of the document (e.g., purpose of the policy, scope, review procedure, etc.)
Policy for general users	Elements that general users of the company must know and/or execute (e.g., physical security, password policy, backup/recovery, etc.)
Policy for system administrator	Elements that must be adopted by the system administrator (e.g., access control procedures, network management, monitoring and logs, etc.)
Policy for database administrator	Elements that must be adopted by the database administrator (e.g., database access management, management of the communication process with the database, management of stored data, etc.)
Audit policy	Elements that must be adopted in the execution of audits (steps and structure of the audit policy, software for audit performs, manual inspection, etc.)

From the "Contextualization" section to "Audit policy" section we use a multiple choice grid with the following scale: 1. not important; 2. slightly important; 3. important; 4. very important; and 5. crucial. This approach guarantees that respondents can easily and quickly answer the questionnaire and they are restricted to a finite set of responses. Additionally, this approach allows the inclusion of more variables in the study, because the format enables the respondents to answer more questions at the same time required to answer few open-ended questions.

The use of a questionnaire to get this data brings us the advantage to reach a high number of small and medium enterprises from different parts of the world. Additionally, the adoption of structured questionnaires are efficient tools that easier data analysis and, at the same, maintaining the anonymity of respondents [29].

However, and despite the benefits mentioned above, there are two typical disadvantages associated with questionnaires that are properly mitigated in this study. In order to mitigate the sampling issues, the questionnaire was available to professionals from different locations. Furthermore, and in order to decrease the probability of getting multiple answers from the same respondent, we collected the IP address of respondent and only the last registered response from the same user was considered as valid.

4. Results

We obtained a total of 144 valid answers, respectively: 20 answers from Chief Executive Officers (CEOs), 36 from Chief Information Officers (CIOs) and 88 from System Administrators (SAs). Around 60% of our respondents are systems administrators. **Table 3** organizes this data for each activity sector. We also look at the size of the company of our respondents. The majority of our respondents (around 40%) come from small companies, which have lesser than 50 employees. **Table 4** summarizes this data grouped by the size of the company.

Table 3. Data frequency organized by industry

Your industry	Your role			Total
	CEO	CIO	SA	
Financial Services	2	5	4	11
Government & Public Sector	3	11	14	28
Health Services	1	8	17	26
Information Technology	10	5	31	46
Manufacturing	3	7	11	21
Tourism	1	0	11	12
Total	20	36	88	144

Table 4. Data frequency organized by size of the company

Size of your company	Your role			Total
	CEO	CIO	SA	
Medium-sized (<250 employees)	3	18	21	42
Micro (<10 employees)	6	2	27	35
Nano-enterprise (<3 employees)	5	0	4	9
Small (<50 employees)	6	16	36	58
Total	20	36	88	144

Looking to the contextualization dimension, the respondents consider that the most important elements are the purpose of the policy (mean is equal to 4,569) and its scope (mean is equal to 4,701). All respondents refer that these two factors are at least important, as stated by the minimum score of 3. The difference is very significant for the other elements of this dimension. Furthermore, the standard deviation is highest for the "review procedure" (std. dev. is equal to 0,911) and is lowest for the "purpose of the policy" (std. dev. is equal to 0,083).

Considering the policy for general users dimension, the respondents state that the top three most relevant elements are: (i) backup/recovery process; (ii) password policy; (iii) email use. In all these variables, the mean is higher than 4. On the other side, the files in system present the lowest mean value. The standard deviation is highest for the "uninterruptible power supplies" (std. dev. is equal to 1,002) and lowest to "files in the system" (std. dev. is equal to 0,633). The amplitude of values is similar to all variables.

The dimension "policy for system administrator" contains 19 questions. The respondents state that the most important variable is the "asset management" followed by the "security risks management" and "backup/recovery process," All these variables present a mean higher than 4,5. Additionally, "change management" and "subcontracting of services" have the highest standard deviation.

The policy for database administrator dimension contains only 3 questions. The data collected reveals that the "management of stored data" was considered the most important element (mean is equal to 4,257). On the other side, the "management of the communication process with the database" is considered the least relevant variable (mean is equal to 2,444). In terms of standard deviation, the "management of the communication process with the database" has the lowest value (std. dev. is equal 0,782).

Finally, the audit policy dimension offers 4 questions. The results indicate that the two most important elements are the "steps and structure of the audit policy" and the "audit survey," The mean of these variables is higher than 4,2). These two variables had also a higher standard deviation. There is a significant difference between the mean of the two most important variables and the others (i.e., "software for audit policy" and "manual inspection"), which present a mean of 2,028 and 1,688, respectively).

The importance of each element in a security policy is depicted in **Fig. 1**. Only the top three most important variable for each dimension were considered. It is possible to conclude that "policy for system administrator" dimension has greater relevance. On the other side, the "policy for database administrator" and "audit policy" have less relevance.

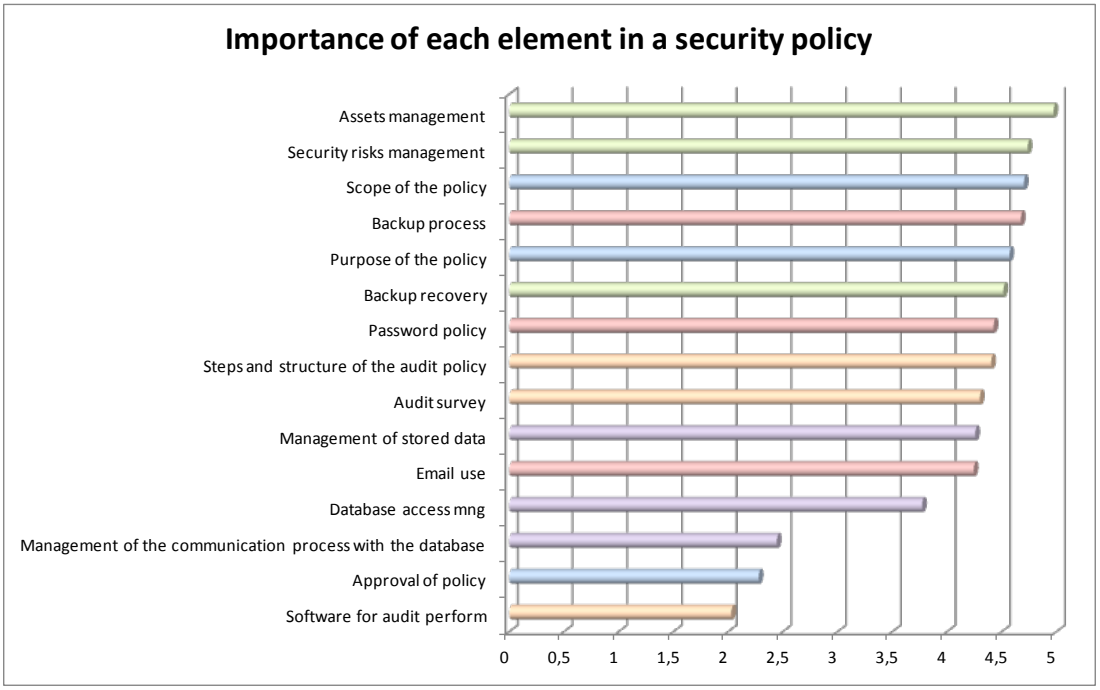

Fig. 1. Analysis of the most important variables for each dimension

Then, we focus our analyzes looking in more detail at the top 25% most important (quartile 3) and to the 25% least important variables (quartile 1). The line cut of quartile 1 is established in 2.1495 and the cut line of quartile 3 is 4.403. After that, we test whether there is enough statistical evidence to conclude that the importance of each variable is different for each activity sector.

4.1 Financial Services Sector

We start by analyzing the least important variables (mean < quartile 1). For that, we perform a two-tailed t-test in order to find evidence of a significant difference between all answers and the respondents from the financial service sector. We adopt a significance level of 5% ($\alpha = 0.05$). Looking at **Table 5** it is possible to conclude that there are three variables with significant mean differences: (i) executive summary; (ii) relation between security and business objectives; and (iii) review procedure.

Table 5. Hypothesis test for the least important variables

Variable	Mean of all answers	Mean in the sector	Pr(|T| > |t|)
Executive summary	1.284	1.727	0.0463
Contacts	1.653	2	0.1682
Manual inspection	1.688	2.182	0.1599

Operating system management	1.75	1.727	0.9095
Relation between security and business objectives	1.792	2.364	0.0184
Review procedure	1.826	2.364	0.0245
Files in the system	1.84	2	0.4210
Penalties	1.965	2.545	0.0927
Software for audit perform	2.028	2.364	0.3038
Web services access management	2.146	1.818	0.1016

We perform the same analysis for the most important variables, which are inside the quartile 3. Looking to **Table 6**, it is possible to conclude that the "scope of the policy" is the only variable that presents a significant mean difference. It was not possible to apply to calculate the t-test for the "assets management" variable because the standard deviation is null.

Table 6. Hypothesis test for the most important variables

Variable	Mean of all answers	Mean in the sector	Pr(|T| > |t|)
Disaster recovery plan	4.403	4.636	0.3613
Steps and structure of the audit policy	4.403	4.273	0.6776
Password policy	4.424	4.818	0.0554
Virus policy management	4.438	4.090	0.2962
Backup/recovery process (SAs)	4.514	4.455	0.8371
Purpose of the policy	4.569	4.818	0.2005
Access control procedures	4.625	4.818	0.3130
Backup/recovery process (GUs)	4.674	4.818	0.4462
Scope of the policy	4.701	4.909	0.0451
Security risks management	4.736	4.636	0.6915
Assets management	4.972	5	N/A

4.2 Government & Public Services Sector

Table 7 shows the results obtained for the two-tailed t-test considering the least important variables for the government & the public services sector. There are three variables that present significant mean differences: (i) contacts; (ii) review procedure; and (iii) penalties.

Table 7. Hypothesis test for the least important variables

Variable	Mean of all answers	Mean in the sector	Pr(|T| > |t|)
Executive summary	1.284	1.571	0.0799
Contacts	1.653	2.214	0.0008
Manual inspection	1.688	1.679	0.9356
Operating system management	1.75	1.893	0.2398
Relation between security and business objectives	1.792	1.929	0.5241
Review procedure	1.826	2.179	0.0490
Files in the system	1.84	1.923	0.3926
Penalties	1.965	2.286	0.0457
Software for audit perform	2.028	2.179	0.0509
Web services access management	2.146	2.286	0.3088

On the other side, and based on **Table 8**, we can conclude that there are five variables that present significant mean differences: (i) disaster recovery plan; (ii) steps and structure of the audit policy; (iii) purpose of the policy; (iv) access control procedures; and (v) scope of the policy.

Table 8. Hypothesis test for the most important variables

Variable	Mean of all answers	Mean in the sector	Pr(|T| > |t|)
Disaster recovery plan	4.403	4.714	0.0287
Steps and structure of the audit policy	4.403	4.714	0.0287
Password policy	4.424	4.5	0.6520
Virus policy management	4.438	4.286	0.4162
Backup/recovery process (SAs)	4.514	4.5	0.9337
Purpose of the policy	4.569	4.929	0
Access control procedures	4.625	4.857	0.0268
Backup/recovery process (GUs)	4.674	4.643	0.8343
Scope of the policy	4.701	4.929	0.0036
Security risks management	4.736	4.857	0.2322
Assets management	4.972	5	N/A

4.3 Health Services Sector

Table 9 presents the results of the same analysis for the health services sector. There are two variables that present significant mean differences: (i) relation between security and business objectives; and (ii) penalties. On the other side, **Table 10** shows the statistical analysis of the most important variables. There are four variables that present significant mean differences: (i) steps and structure of the audit policy; (ii) purpose of the policy; (iii) access control procedures; and (iv) scope of the policy.

Table 9. Hypothesis test for the least important variables

Variable	Mean of all answers	Mean in the sector	Pr(|T| > |t|)
Executive summary	1.284	1.231	0.5333
Contacts	1.653	1.846	0.1205
Manual inspection	1.688	1.846	0.0946
Operating system management	1.75	1.692	0.5969
Relation between security and business objectives	1.792	2.154	0.0113
Review procedure	1.826	2.269	0.0681
Files in the system	1.84	2.038	0.1034
Penalties	1.965	2.231	0.0295
Software for audit perform	2.028	2.192	0.1006
Web services access management	2.146	2.154	0.9621

Table 10. Hypothesis test for the most important variables

Variable	Mean of all answers	Mean in the sector	Pr(|T| > |t|)
Disaster recovery plan	4.403	4.462	0.7442
Steps and structure of the audit policy	4.403	4.769	0.0083
Password policy	4.424	4.385	0.8328
Virus policy management	4.438	4.269	0.4164
Backup/recovery process (SAs)	4.514	4.385	0.4899
Purpose of the policy	4.569	4.923	0.0001
Access control procedures	4.625	4.846	0.0484
Backup/recovery process (GUs)	4.674	4.615	0.7132
Scope of the policy	4.701	4.923	0.0079
Security risks management	4.736	4.769	0.7970
Assets management	4.972	4.923	0.5306

4.4 Information Technology Sector

Table 11 presents the results of the same analysis for the information technology (IT) sector. In this case, there are seven variables that offer significant mean differences: (i) executive summary; (ii) contacts; (iii) manual inspection; (iv) relation between security and business objectives; (v) review procedure; (vi) penalties; and (vii) web services access management. On the other side, **Table 12** presents a similar analysis of the most important variables. The "steps and structure of the audit policy" is the only element that presents a significant mean difference.

Table 11. Hypothesis test for the least important variables

Variable	Mean of all answers	Mean in the sector	Pr(|T| > |t|)
Executive summary	1.284	1.109	0.005
Contacts	1.653	1.304	0
Manual inspection	1.688	1.478	0.0126
Operating system management	1.75	1.891	0.2002
Relation between security and business objectives	1.792	1.5	0.0027
Review procedure	1.826	1.435	0.0002
Files in the system	1.84	1.739	0.3623
Penalties	1.965	1.457	0
Software for audit perform	2.028	1.87	0.0535
Web services access management	2.146	2.478	0.0078

Table 12. Hypothesis test for the most important variables

Variable	Mean of all answers	Mean in the sector	Pr(|T| > |t|)
Disaster recovery plan	4.403	4.109	0.0607
Steps and structure of the audit policy	4.403	4.043	0.0199
Password policy	4.424	4.283	0.3444
Virus policy management	4.438	4.609	0.1559
Backup/recovery process (SAs)	4.514	4.609	0.4275
Purpose of the policy	4.569	4.348	0.1205

Access control procedures	4.625	4.348	0.1634
Backup/recovery process (GUs)	4.674	4.717	0.6967
Scope of the policy	4.701	4.522	0.1655
Security risks management	4.736	4.739	0.9753
Assets management	4.972	5	N/A

4.5 Manufacturing Sector

Table 13 presents the results for the manufacturing sector. In this situation, there are two variables that demonstrate to have significant mean differences: (i) penalties; and (ii) web services access management. On the other side, there are no evidences that any of the variables listed in **Table 14** have significant mean differences.

Table 13. Hypothesis test for the least important variables

Variable	Mean of all answers	Mean in the sector	Pr(|T| > |t|)
Executive summary	1.284	1.286	0.9866
Contacts	1.653	1.571	0.5865
Manual inspection	1.688	1.857	0.2503
Operating system management	1.75	1.524	0.2173
Relation between security and business objectives	1.792	1.714	0.6249
Review procedure	1.826	1.714	0.4836
Files in the system	1.84	1.714	0.3164
Penalties	1.965	2.380	0.0180
Software for audit perform	2.028	1.952	0.3778
Web services access management	2.146	1.761	0.0330

Table 14. Hypothesis test for the most important variables

Variable	Mean of all answers	Mean in the sector	Pr(|T| > |t|)
Disaster recovery plan	4.403	4.476	0.7359
Steps and structure of the audit policy	4.403	4.429	0.9005
Password policy	4.424	4.524	0.6060
Virus policy management	4.438	4.524	0.6572
Backup/recovery process (SAs)	4.514	4.429	0.6769
Purpose of the policy	4.569	4.333	0.2769
Access control procedures	4.625	4.810	0.1752
Backup/recovery process (GUs)	4.674	4.619	0.7576
Scope of the policy	4.701	4.619	0.6458
Security risks management	4.736	4.714	0.8910
Assets management	4.972	5	N/A

4.6 Tourism Sector

Finally, **Table 15** presents the results for the tourism sector. In this scenario, there are five variables that demonstrate to have significant mean differences: (i) contacts; (ii) relation between security and business objectives; (iii) review procedure; (iv) penalties; and (v) web

services access management. On the other side, only the "access control procedures" variable presents significant mean differences looking in **Table 16**.

Table 15. Hypothesis test for the least important variables

Variable	Mean of all answers	Mean in the sector	Pr(|T| > |t|)
Executive summary	1.284	1	N/A
Contacts	1.653	1.083	0
Manual inspection	1.688	1.417	0.0952
Operating system management	1.75	1.417	0.1121
Relation between security and business objectives	1.792	1.417	0.0282
Review procedure	1.826	1.25	0.0083
Files in the system	1.84	1.667	0.2482
Penalties	1.965	1.333	0.0010
Software for audit perform	2.028	1.75	0.2277
Web services access management	2.146	1.5	0.0068

Table 16. Hypothesis test for the most important variables

Variable	Mean of all answers	Mean in the sector	Pr(|T| > |t|)
Disaster recovery plan	4.403	4.333	0.8109
Steps and structure of the audit policy	4.403	4.333	0.8109
Password policy	4.424	4.333	0.7557
Virus policy management	4.438	4.667	0.3308
Backup/recovery process (SAs)	4.514	4.667	0.5110
Purpose of the policy	4.569	4	0.0858
Access control procedures	4.625	3.833	0.0221
Backup/recovery process (GUs)	4.674	4.667	0.9746
Scope of the policy	4.701	4.333	0.2224
Security risks management	4.736	4.5	0.3855
Assets management	4.972	4.833	0.4231

5. Discussion

The top 3 most important components of a security policy stated by our respondents are: (i) asset management; (ii) security risk management; and (iii) scope of the policy. Their standard deviation is different. The low value of the standard deviation for the "assets management" variable indicates that the large majority of our respondents consider it very relevant. The other two variables are also very important, but this opinion is not so unanimous among all the respondents.

The asset management includes all practices that are used to ensure that all the IT assets are properly allocated to end-users. The idea is to guarantee the simplification of technical support and maintenance requirements. It involves the right balancing of costs, opportunities and risks against the desired performance of assets, to achieve the organizational objectives. The registration of assets can be done using a QR code in order to register the technical information of the asset and its conditions of access and use. The equipment must be validated and updated periodically (e.g., 3 months, 6 months, etc.) to guarantee a constant update of the components,

and also to check if something is missing.

The security risk management has the main challenge to protect the information inside the company. The information, in its most varied forms, is one the most valuable and strategic assets of any company today. The Information security is based on six pillars: (i) confidentiality; (ii) integrity; (iii) availability; (iv) authentication; (v) non-repudiation; and (vi) auditability. Therefore, risk management can be seen as a dynamic, continuous and essential process for the good governance of any organization. As a consequence, an organization must have the capacity and competence to diagnose, prioritize, monitor and treat their risks, always attentive to changes in the internal and external environment, to not be surprised by unknown or uncontrolled risks.

The scope of the policy appears in the contextualization dimension and is one of the most important basic elements of an IT security policy. Together with the purpose of the policy, it is considered the two most important elements of the contextualization dimension. The scope of the policy has the responsibility to establish who the policy applies to. Some security policies may be related to everyone in the organization (e.g., password policy, use of external devices, etc.) and others may be specific to how the IT department will handle the communication, such as the system update policy. Organizations may break policies into different categories, to better reflect their organizational structure and culture.

On the other side, the top 3 least important elements of an IT security plan are: (i) executive summary; (ii) contacts; and (iii) manual inspection. This situation is mainly explained due to the current dynamic nature of companies. The traditional organization in several departments/silos is becoming loosing importance and emerge the organization of the company and its work by functional areas.

The importance given to some elements of the security policy is not uniform for all activity sectors. In the financial sector, the executive summary, the relation between security and business objectives, the review procedure, and the scope of the policy are considered more important than the average. This situation is mainly due to a greater formalism in financial sector companies, which make these companies more focused on internal processes.

In the government & public services sector, we find that a total of eight variables present significant mean differences. Elements, such as contacts, penalties or access control policies assume a more important role. This sector of activity is recognized as an area where institutions assume a larger dimension, and in which aspects related to processes and bureaucracy are well established.

In the Health Services Sector there are six variables that present significant mean differences. The majority of these elements are similar to government & public services sector, where penalties, steps and structure of the audit policy, the purpose of the policy, and access control policies are elements that have more relevance.

In the IT field, we find a total of eight elements that present significant mean differences. However, seven of these eight elements are related to the least important variables. In fact, elements such as an executive summary, contacts, manual inspection, and penalties assume less importance. On the other side, web services access management is considered more important in the IT field. The IT field is characterized by having smaller companies (e.g., nano-enterprises and micro companies). In this sense, institutions become more dynamic and market oriented, adopting agile methodologies in the development of their projects, hence the formalisms instituted have to be essentially more reactive.

The manufacturing sector is essentially a more traditional sector. Only two elements appear to present significant mean differences. One of them is the penalties that assume more

importance, and the other is the web services access management that shows less importance.

Finally, the tourism sector has six elements (e.g., contacts, review procedure, penalties or access control policies) that present significant mean differences. The tourism sector is still a very young sector of activity that has grown exponentially in several countries and, therefore, its companies are essentially dynamic. However, unlike the IT field, there is a lesser enthusiasm for the technology field, hence the establishment of an access policy is considered less relevant. This situation may be critical from a medium to long-term perspective, considering that tourism companies have a greater number of seasonal workers, turning systems vulnerable to misuse, whether intentional or not, by new employees.

6. Conclusion

The information is an asset that must be protected and cared by the rules and procedures defined as security policies, in the same way that we protect our financial and patrimonial resources. The information security policy is the document that guides and establishes the guidelines of an organization for the protection of information assets and the prevention of legal liability for all users. This policy must be applied across all areas of the institution. Likewise, SMEs also need to implement these security policies, which may otherwise jeopardize their entire business and, consequently, their operational and financial viability.

Through this study, it was possible to identify the most important and the least relevant elements in the structure of a security policy. Additionally, the study revealed that the relative importance of these elements is slightly changed according to the sectors of activity. It is important for SMEs to be aware of these elements in order to design their security policies in a precise, concise and unambiguous way.

References

[1] IC3, "Internet Crime Report," Internet Crime Complaint Center, 2012. Available in: https://pdf.ic3.gov/2012_IC3Report.pdf (accessed on 6th of December 2016).

[2] A. Sword, "SMEs hit with 7 million cyber crime attacks per year in £5.26 billion blow to UK economy," *Computer Business Review*, 2016. Available in: http://www.cbronline.com/news/cybersecurity/business/smes-hit-with-7-million-cyber-crime-attacks-per-year-in-526-billion-blow-to-uk-economy-4919992/ (accessed on 6th of December 2016).

[3] D. Beley, and P. Bhatarkar, "The Role of Information Technology in Small and Medium Sized Business," *International Journal of Scientific and Research Publications*, 3(2), pp. 1-4, 2013. Article (CrossRef Link).

[4] F. Korcek, V. Bolek, and M. Benova, "Security of Information Assets in Small and Medium-sized Enterprises," *Economic Review*, 45, pp. 45-55, 2016. Article (CrossRef Link).

[5] M. Umar, A. Mehmood, and H. Song, "SeCRoP: secure cluster head centered multi-hop routing protocol for mobile ad hoc networks," *Security and Communication Networks*, 9(16), pp. 3378-3387, 2016. Article (CrossRef Link).

[6] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, 4, pp. 2840-2853, 2016. Article (CrossRef Link).

[7] S. Shamshirband, S. Kalantari, Z. Daliri, and L. Shing, "Expert security system in wireless sensor networks based on fuzzy discussion multi-agent systems," *Scientific Research and Essays*, 5(24), pp. 3840-3849, 2010. Article (CrossRef Link).

[8] C. Manso, E. Rekleitis, F. Papazafeiropoulos, and V. Maritsas, "Information security and privacy standards for SMEs," ENISA, 2015. Available in: https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport
[9] S. Shamshirband, M. Shojafar, A. Hosseinabadi, M. Kardgar, M. Nasir, and R. Ahmad, "OSGA: genetic-based open-shop scheduling with consideration of machine maintenance in small and medium enterprises," *Annals of Operations Research*, 229(1), pp. 743-758, 2015. Article (CrossRef Link).
[10] A. Hosseinabadi, H. Siar, S. Shamshirband, M. Shojafar, and M. Nizam, "Using the gravitational emulation local search algorithm to solve the multi-objective flexible dynamic job shop scheduling problem in Small and Medium Enterprises," *Annals of Operations Research*, 229(1), pp. 451-474, 2015. Article (CrossRef Link).
[11] D. Lacey, and B. James, "Review of Availability of Advice on Security for Small/Medium Sized Organisations," ICO, 2010. Available in: http://ico.org.uk/about_us/research/~/media/documents/library/Corporate/Research_and_reports/REVIEW_AVAILABILITY_OF_%20SECURITY_ADVICE_FOR_SME.pdf
[12] A. Tawileh, J. Hilton, and S. McIntosh, "Managing information security in small and medium sized enterprises: a holistic approach," in *Proceedings of the ISSE/SECURE*, pp. 331–339, 2007. Article (CrossRef Link).
[13] Z. Soomro, M. Shah, and J. Ahmed, "Information security management needs more holistic approach: A literature review," *International Journal of Information Management*, 36(2), pp. 215-225, 2016. Article (CrossRef Link).
[14] J. Park, R. Robles, C. Hong, S. Yeo, and T. Kim, "IT Security Strategies for SME's," *International Journal of Software Engineering and Its Applications*, 2(3), pp. 91-98, 2008. Article (CrossRef Link).
[15] J. Abbas, H. Mahmood, and F. Hussain,"Information Security Management for Small and Medium Enterprises," *Science International*, 27(3), pp. 2393-2398, 2015. Article (CrossRef Link).
[16] H. Kluitenberg, "Security Risk Management in IT Small and Medium Enterprises," in *Proceedings of 20th Twente Student Conference on IT*, Twente, Netherlands, 2014. Article (CrossRef Link).
[17] N. Amrin, "The Impact of Cyber Security on SMEs," MSc. thesis in Electrical Engineering, Mathematics and Computer Science, University of Twente, 2014. Available in: http://essay.utwente.nl/65851/
[18] K. Renaud, "How smaller businesses struggle with security advice," *Computer Fraud & Security*, 2016(8), pp. 10-18, 2016. Article (CrossRef Link).
[19] A. Santos-Olmo, L. Sánchez, I. Caballero, S. Camacho, and E. Fernandez-Medina, "The Importance of the Security Culture in SMEs as Regards the Correct Management of the Security of Their Assets," *Future Internet*, 8(30), pp. 1-27, 2016. Article (CrossRef Link).
[20] M. Alshaikh, S. Maynard, A. Ahmad, and S. Chang, "Information Security Policy: A Management Practice Perspective," in *Proc. of the Australasian Conference on Information Systems*, Adelaide, Australia, pp. 1-13, 2015. Article (CrossRef Link).
[21] T. Peltier, "Implementing an information security awareness program," *Information Systems Security*, 14(2), pp. 12-37, 2005. Article (CrossRef Link).
[22] I. Lopes, and P. Oliveira, "Implementation of information systems security policies: A survey in small and medium sized enterprises," in *Proc. of World Conference on Information Systems and Technologies*, Ponta Delgada, Portugal, pp. 459-468, 2015. Article (CrossRef Link).
[23] I. Lopes, and Sá-Soares, "Information security policies: A content analysis," in *Proc. of 16th Pacific Asia Conference on Information Systems*, Ho Chi Minh City; Vietnam, 2012. Article (CrossRef Link).
[24] M. Sadok, and P. Bednar, "Information Security Management in SMEs-Beyond the IT challenges," in *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, pp.209-219, 2016. Article (CrossRef Link).
[25] J. Alqatawna, "The Challenge of Implementing Information Security Standards in Small and Medium e-Business Enterprises," *Journal of Software Engineering and Applications*, 7, pp. 883-890, 2014. Article (CrossRef Link).

[26] H. Cholez, and F. Girard, "Maturity assessment and process improvement for information security management in small and medium enterprises," *Journal of Software: Evolution and Process*, 26(5), pp. 496-503, 2014. Article (CrossRef Link).
[27] F. Mijnhardt, T. Baars, and M. Spruit, "Organizational Characteristics Influencing SME Information Security Maturity," *Journal of Computer Information Systems*, 56(2), pp. 106-115, 2016. Article (CrossRef Link).
[28] S. Sukamolsen, "Fundamentals of quantitative research," Language Institute, Chulalongkorn University, Bangkok, Thailand, 2010. Article (CrossRef Link).
[29] M. Zohrabi, "Mixed Method Research: Instruments, Validity, Reliability and Reporting Findings," *Theory and Practice in Language Studies*, 3(2), pp. 254-262, 2013. Article (CrossRef Link).

Fernando Almeida has a PhD. in Computer Science Engineering. He has more than 15 years of experience in the fields of software engineering, computer networks and information security. His current research interests include security policies, agile software practices and technological entrepreneurship.

Inês Carvalho has a B.E. in Computer Systems and Network. She has experience in the field of networks security, information systems and software development. In the future, she intends to continue to carry out research and business work in these areas.

Fábio Cruz has also a B.E in Computer Systems and Network. He has experience in the field of computer networks management and system administration. In the future, he intends to continue to carry out research and business work in these areas.