International Journal of Information Systems and Software Engineering for Big Companies (IJISEBC)

Recibido: 07-12-2017 / Revisado: 13-12-2017
Aceptado: 13-12-2017 / Publicado: 15-12-2017

IJISEBC, 4(2), 2017

Cybersecurity culture in Portuguese organizations: an exploratory analysis

La cultura de la ciberseguridad en las organizaciones portuguesas: un análisis exploratorio

Margarida G. M. S. Cardoso[1], Rosário D. Laureano[1], Carlos Serrão[1]

[1] Instituto Universitário de Lisboa (ISCTE-IUL), Portugal

margarida.cardoso@iscte.pt , maria.laureano@iscte.pt , carlos.serrao@iscte.pt

ABSTRACT. Cybersecurity is currently one of the hottest topics for millions of organizations around the world. They depend on information technology to conduct their business processes that are exposed to wide range of security threats, and Portuguese organizations are no exception. How are these organizations taking a holistic approach to allow them to face and handle those threats with confidence? Are the proper technical mechanisms being put in place and are the appropriate information security skills and awareness programs implemented internally? How is all of this being handled by Portuguese organizations? This are some of the questions tackled on a survey addressed to directors of Portuguese organizations in order to map their current cybersecurity culture and corresponding processes. .

RESUMEN. La ciberseguridad es actualmente uno de los temas más candentes para millones de organizaciones en todo el mundo. Dependen de la tecnología de la información para llevar a cabo sus procesos de negocio que están expuestos a una amplia gama de amenazas a la seguridad, y las organizaciones portuguesas no son una excepción. ¿Cómo estas organizaciones están adoptando un enfoque holístico para permitirles enfrentar y manejar esas amenazas con confianza? ¿Se están implementando los mecanismos técnicos adecuados y se implementan internamente las habilidades de seguridad de la información y los programas de concienciación adecuados? ¿Cómo es todo esto manejado por organizaciones portuguesas? Estas son algunas de las preguntas abordadas en una encuesta dirigida a directores de organizaciones portuguesas para trazar su actual cultura de ciberseguridad y los procesos correspondientes.

KEYWORDS: Cybersecurity, Portuguese, Study, Organizations, Practices, Challenges.

PALABRAS CLAVE: La seguridad cibernética, Portugués, Estudio, Organizaciones, Prácticas, Desafíos.

Cardoso, M. G. M. S.; Laureano, R. D.; Serrão, C. (2017). Cybersecurity culture in Portuguese organizations: an exploratory analysis. *International Journal of Information Systems and Software Engineering for Big Companies (IJISEBC)*, 4(2), 23-30.

1. Introduction

The growing number of organizations that are dependent of information and communication technologies (ICT) to conduct their business processes is increasingly larger. ICT allows businesses to be more efficient, offer better services to customers, provide better process integration with partners and suppliers and develop new products. However, all of these ICT-powered opportunities are followed by much bigger challenges. One of the most relevant challenges organizations have to face nowadays concerns the growing number of menaces that this digital infrastructure has to endure and the investment necessary to provide the required protection measures that will allow its flawless operation (Dutta & McCrohan, 2002).

The security challenges (Whitman, 2003) that organizations face currently raise questions about the extent to which organizations are ready to tackle them (Zhu, 2009). These questions are relevant, not only from a purely technical perspective (that is, to what extent organizations have the technical means to address security challenges) but also from other perspectives such as organizational awareness of these challenges and the knowledge needed to recognize and address them (Puhakainen & Siponen, 2010).

Thus, it is important to understand, in particular in the Portuguese context, how cybersecurity is tackled, and what measures Portuguese organizations take (or intend to take in the near future) to address the possible challenges they face, and how they are aligned with the best practices that are carried out by their European counterparts or globally (Bodeau, Graubart & Fabius-Greene, 2010).

Usually, as a result of the difficulties associated with estimating the benefits from cybersecurity investments, there is a widespread belief that private sector firms tend to underinvest in cybersecurity activities (Desman, 2001). Furthermore, firms tend to defer much of their cybersecurity investments unless reacting to a major cybersecurity breach. That is, firms tend to take a reactive, rather than proactive approach toward cybersecurity investments related to their organizations.

This work represents one of the first Portuguese organizations studies regarding their approach to cybersecurity. It was carried out jointly with the cooperation of the Portuguese Association for the Promotion of Information Security (AP2SI), with the national organizations main stakeholders and decision maker's collaboration.

In this paper, we start by providing this introduction to the theme, contextualize and present its main motivations. The following section refers to the research instrument – an online survey. The third section highlights some of results on key-issues at work.

Finally, the last section of this paper draws the main conclusions of this study and indicates future research perspectives.

2. Survey on cybersecurity practices

In order to obtain specific information concerning the Portuguese organizations reality in Information Security (IS), namely to realize how they understand the IS theme and how they put it into practice, it was conducted a study that helped the identification of this reality (Bulgurcu, Cavusoglu & Benbasat, 2010). Also, this study can serve as a reference to raising awareness to the IS topic in organizations operating in Portugal. The study envisaged not only those responsible for IT or security in organizations, but also other employees - in order to construct a more complete view of the existing perception. As IS threats become more commonplace and present in people's day-to-day lives, it is important to realize how organizations are responding to the challenges, not only technologically but, perhaps even more important, culturally and organizationally.

The research instrument used was a survey covering fundamental aspects to the understanding of the IS culture in Portuguese organizations. It was conducted online between July 2015 and September 2015. All

those working in institutions, with some direct or indirect responsibilities in the IS field, located in Portuguese territory were invited to participate. The target respondents should exert management functions in the organization (in what follows they will be referred to as directors) in order to provide more valuable insights through the questionnaire.

The topics to be addressed included: the top management commitment to the theme; skills training; the existence of a dedicated organizational unit; the role of audit and control; and the management of security threats and incidents. It was also found necessary to deepen some of the issues from the directive and management layers' viewpoint, specifically on: the management of the IS budget; the human resources management with functions in Information Security; the existence and eventual losses related to incidents; the safety concerns of top management; the perception of the institution's exposure to threats.

Most of measurement scales used are qualitative and the expression of opinions are being recorded in Likert type scales (Likert, 1932) "– e.g from 1 extremely likely, 2, 3, 4, 5- not likely or 1- much concern, 2, 3, 4, 5- less concern. We note that, in the next section, the percentages generally refer to the valid responses, which do not necessarily coincide with the total number of respondents. Whenever it is convenient, in order to clarify the results, we present counts instead of percentages

3. Questions and answers

In the present study we report the data analysis referring to 59 respondents to the questionnaire that exert management positions – e.g. CEO (Chief Executive Officer), CIO (Chief Information Officer), CTO (Chief Technology Officer), CSO (Chief Security Officer) or CFO (Chief Financial Officer, Director of Audit, Risk, Compliance and Internal Control, and other steering functions. Most of them are employees in telecommunications services and information technologies organizations (14) and also on investigation and security provision of private security services organizations (12). In general, the organizations considered are either very small in terms of volume of business (16 are below 2,000,000 €/year) or very large (13 are above 500,000,000€/year), with some of the medium size companies being scattered by diverse volumes in between. The size referring to the number of employees is illustrated in Figure 1.

A. Information Security

The respondents distinguish the contractual definition of responsibilities of employees regarding IS in specific functions (15) or all functions (21). However, these contractual responsibilities do not exist in 18 cases.

In 30 cases, the responses indicate that IS objectives are defined for employees.

The concern of top management with the IS is affirmed by the majority of respondents, but only in 13 responses from directors it is stated that the organization is certified in some IS management standard.

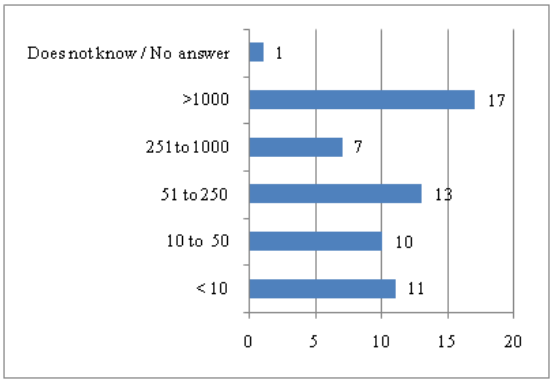

Figure 1. How many employees are there in your organization?

B. Information Security Policy

The existence of an IS policy is confirmed in 40 cases. To these respondents who claim there is an IS policy was required to answer 5 additional questions to characterize this policy. The answers are summarized in Table I.

	Frequency
1.**The IS policy is issued by the top management of organization**	31
2.**Support from top management to the IS policy** is materialized in:	
Followingtheidentifiedguidelines	21
by participating in a security committee or similar	13
by personally appealing to their implementation	18
by participating in training and awareness actions	11
3.**The revision of IS policy** is carried out:	
whenever there are changes in the organization	17
once per year	15
4.**Knowledge of IS policy** is stated by directors	26
5.**The sharing of IS policy** is:	
not shared outside the organization	15
shared with the customers	15

Table 1. IS Policy,

Almost half of the directors state that the institution does perform periodic actions to raise employees IS awareness (e.g.: posters, newsletters, videos, games, other non-training activities); 26 of them state otherwise.

C. Training program

It is stated by most respondents (30 directors) that the organization does not have a training program in IS for employees (e.g.: classroom training, outside classroom training, knowledge assessment).

The 15 directors who claimed the existence of an IS training program at the organization were questioned about the characterization of this program: only 8 claim that the IS training is mandatory in the organization and 9 state that the IS training is regularly given to all employees. The themes addressed in the IS training are mainly "Good practices in the use of information systems" (14), "How to act in the case of incident detection" (13) and "Good practices in handling information" (12).

D. Structure

About half of the directors state that the organization does not have a specific IS-structure while the same percentage reports the opposite. The latter are questioned if the IS-structure reports directly to the top management of organization and 16 respond affirmatively.

According to 31 directors, the IS activities are included in the area responsible for the management of information systems.

A high number of directors (13) does not know or does not answer about the characterization of the annual budget of the organization allocated to IS. The majority (11 responses) considers it "Less than 1% of the organization's budget" (Figure 2).

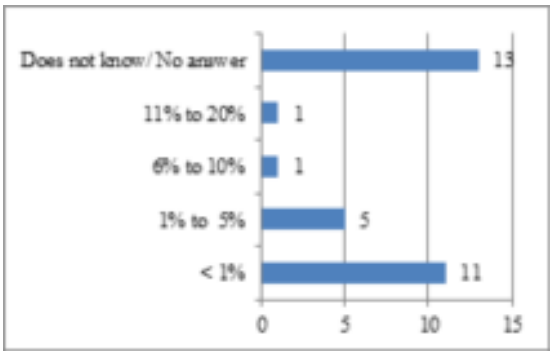

Figure 2. Percentage of organization budget applied to IS.

About half of respondents anticipate that the IS budget for next year should remain unchanged. As for the method used to analyze the return on IS investment, the majority (18) states that no method is used (Table 2). The 22 directors who stated there was an IS-structure on the organization were questioned about the existence of a specific budget for IS. The number of affirmative answers (9) is equal to the number of negative ones. Among the negative answers, only 3 claim that the IS budget is incorporated into the information systems' budget. The intent to establish a specific IS budget for the next year is indicated only by 4 directors only, and 6 directors state that no method is used to analyze the IS return on investment.

Some respondents (29) report the existence of employees dedicated to IS issues. Three additional issues were posed to these respondents – see Table 3.

	Frequency
ROI - Return on Investment	2
IRR - Internal Rate of Return	1
No method	18
Does not know/No answer	9
Other (please specify)	1
Total	31

Table 2. Analysis of IS return on investment.

1.What percentage of professionals dedicated to IS are certified?	**Frequency**
Our professionals are not certified	6
< 25%	9
26% to 50%	1
51% to 75%	0
> 75%	4
Does not know/ No answer	9
2.What percentage of outsourcing is used in IS?	
Thereis no outsourcing	10
< 25%	7
26% to 50%	3
51% to 75%	0
> 75%	1
Does not know/ No answer	8
3.Rate the ease of hiring specialized professionals in IS	
Veryeasy	0
Reasonably easy	2
Neither easy nor difficult	3
Reasonably difficult	9
Very difficult	7
Does not know/ No answer	8

Table 3. Professionals dedicated to IS.

E. Audits

According to 25 directors, IS audits are carried out in their organization. The regularity with which they are carried out is essentially "Once a year" (8) or "More than once a year" (10). Most directors (24) state that the institution tests the implemented security controls (Figure 3).

Some respondents (28) said the organization contemplates the inclusion of IS clauses in contracts with

suppliers and 32 state that the organization does not perform IS audits to suppliers.

F. Incidents

Some respondents (19) believe that the organization has the capacity to detect and respond in time only to "Simple incidents". Some directors (14) also believe that complex incidents can be dealt with by the organization.

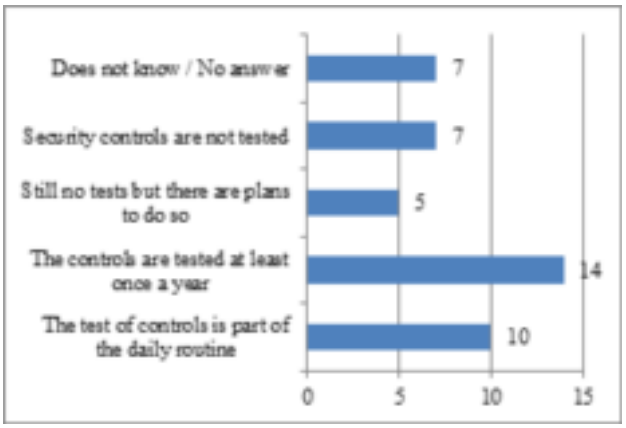

Figure 3. Does the institution test the implemented security controls?

Most directors (14) indicate that the number of IS incidents detected last year is below 10. There are 15 directors who do not know the answer, while 17 do not provide any answer at all.

G. Threats

Only 10 directors state that they have been targeted by an IS attack. In general, the directors (30) are aware of the procedures in place in the organization to act in the case of being victim of an attack. The probability of the organization to fall victim to an attack next year (scale ranges from "1-very unlikely" to "5-very likely") is viewed as almost uniformly distributed among the 2 to 5 levels (only 5% consider the attack very unlikely).

The "Attacks on Internet sites of the institution" and the "Malicious software" are the most frequent type of IS incidents that were detected by the institution – Table 4.

About the identification of the actors involved in IS incidents they are mainly referred to "Hackers nonaligned with criminal organizations" – Table 5.

The degree of concern with diverse (16) IS issues is established, by 42 respondents, in a 5 points scale: from "1 least concern" to "5-much concern". A summary of results obtained is presented in Table 6.

	N	Percent	Percent of Cases
Illegal access to sensitive data	8	8.7%	29.6%
Threats related to the supply chain	7	7.6%	25.9%
Attacks on Internet sites of the institution	14	15.2%	51.9%
Collaborator's malicious activity	8	8.7%	29.6%
Social engineering	8	8.7%	29.6%
Hacking or network intrusion	13	14.1%	48.1%
Loss or theft of mobile devices	6	6.5%	22.2%
Phishingorspearphishing	13	14.1%	48.1%
Malicious software (viruses, worms, Trojan horses, etc.)	15	16.3%	55.6%

Table 4. Which IS incidents were detected by the organization.

	N	Percent	Percent of Cases
Nations	4	7.1%	16.7%
Malicious collaborators	12	21.4%	50.0%
Non-malicious collaborators	10	17.9%	41.7%
Hackers nonaligned with criminal organizations	15	26.8%	62.5%
Hacktivists	6	10.7%	25.0%
Criminal organizations	9	16.1%	37.5%

Table 5. Identify (as much as possible) the factors involved in threats to IS in the organization.

	Levelofconcern	Frequency
Hacker attacks or criminal organizations	4	10
	Much concern	13
Attacks that compromise the service through business channels and customer communication	4	10
	Much concern	12
Cloud computing	Less concern	11
	3	12
Compliance with laws and other regulations	4	15
	Much concern	9
Unawareness of threats	4	10
	Much concern	13
Unauthorized public dissemination of the institution's information	3	11
	Much concern	15
Lack of attack detection capability	3	9
	4	9
	Much concern	14
Lack of fiscal capacity	2	9
	3	13
Lack of specialized staff	2	10
	3	10
	4	10
Inability to ensure service to customers	4	8
	Much concern	18
Unavailability of essential systems to business	4	11
	Much concern	16
Protection of personal data and sensitive personal data	3	12
	Much concern	14
Theft of business information / intellectual property	3	10
	Much concern	15
Security in the supply chain (services and products)	Lessconcern	9
	3	16
	4	9
Shadow IT (systems used by the institution but unknown to the IS management area)	2	12
	3	11
Malicious software (viruses, worms, Trojan horses, etc.)	3	10
	4	16

Table 6. IS issues that most concern the organization.

4. Conclusions

Information security is one of top priorities of organizations as a way to preserve and protect their intangible assets. Organizations face today enormous challenges represented by asymmetric menaces that target their private information and therefore need to design and invest in the appropriate strategies to implement countermeasures against those. In an effort to capture and understand the Portuguese reality, it was conducted a study addressing a set of medium sized and large companies, in order to understand their strategy concerning cybersecurity.

The analysis of the survey conducted suggests that in the Portuguese organizations the top management is knowledgeable about some of the topics covered and is aware of some risks in the information security field. However, the results obtained suggest that, for some organizations top management, these risks still do not justify the adoption of specific measures such as the hiring of specialized personnel or the creation of specific IS-structures within the institutions which can be entirely dedicated to the information security subject. In fact, only 29 respondents reported the existence of employees dedicated to IS issues and the creation of specific IS structures occurs in only half of studied organizations.

The organizations that can build capacity to analyze and perceive the new IS threats will be working not only to improve their security but also to streamline the way they are embedded in the economic, social and technological environment (Whitman, 2003). It is important to emphasize that the ways in which information is transmitted and stored evolve more and more rapidly, and institutions that are unable to adapt to these changes, which are also cultural, may be putting their future at risk. This study reveals that some Portuguese companies, by their lack of adaptation and strategy towards information security, may fall under this stereotype.

The study presented some interesting results, in particular about the maturity of Portuguese institutions towards the information security challenges (Lessing, 2008). However, its conclusions refer only to the data collected in a single year period study which only provides a static view. A more dynamic view will be provided in the future, since the survey will be conducted every year with a growing sample, including all of the organizations' collaborators. This will allow the capture a more dynamic perspective on the evolution of the information security maturity of Portuguese organizations, in particular to what concerns observing the different attitude of Portuguese organizations towards the growing information security threats affecting the digital landscape.

Acknowledgements

The authors of this article would like to acknowledge and thank the work conducted by the Portuguese Association for the Promotion of Information Security (AP2SI), pushing the survey to Portuguese companies. Also, we would like to thank to all the organizations that collaborated in this study.

Cómo citar este artículo / How to cite this paper

Cardoso, M. G. M. S.; Laureano, R. D.; Serrão, C. (2017). Cybersecurity culture in Portuguese organizations: an exploratory analysis. *International Journal of Information Systems and Software Engineering for Big Companies (IJISEBC)*, 4(2), 23-30. (www.ijisebc.com)

References

Bodeau, D. J.; Graubart, R.; Fabius-Greene, J. (2010). Improving Cyber Security and Mission Assurance Via Cyber Preparedness (Cyber Prep) Levels. In IEEE Second International Conference on Social Computing (1147-1152).

Bulgurcu, B.; Cavusoglu, H.; Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q., 34(3), 523-548.

Desman, M. B. (2001). Building an Information Security Awareness Program. CRC Press.

Dutta, A.; McCrohan, K. (2002). Management's role in information security in a cyber economy. Calif. Manage. Rev., 45(1), 67-87.

Lessing, M. M. (2008). Best practices show the way to Information Security Maturity. In 6th National Conference on Process Establishment, Assessment and Improvement in Information Technology (ImproveIT 2008) (1-9).

Likert, R. (1932). A Technique for the measurement of attitudes. Archives of Psychology, 140, 1-55.

Puhakainen, P.; Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. Mis Q., 34(4), 757-778.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. Commun. ACM, 46(8), 91-95.

Zhu, H. (2009). Towards a Theory of Cyber Security Assessment in the Universal Composable Framework. In 2009 Second International Symposium on Information Science and Engineering (203-207).