CAPSI 2019 Proceedings

Portugal (CAPSI)

10-2019

The Role of the Chief Information Security Officer (CISO) in Organizations

Pedro Monzelo

Sérgio Nunes

The Role of the Chief Information Security Officer (CISO) in Organizations

Pedro Monzelo, ISEG – UL, Portugal, pedro_monzelo89@hotmail.com
Sérgio Nunes, ISEG – UL, Portugal, snunes@iseg.ulisboa.pt

Abstract

In an increasingly connected and digital world, information is seen as a business enabler and source of sustained competitive advantage. Thus, information security is becoming critical to protect these information assets, which is why organizations' information security strategy has been aligning with their strategic goals. This paper aims to study organizations' general information security environment, analyse the CISO's role in them and understand where they should be positioned on the organizational structure. Interviews were conducted on experienced information security consultants, information systems and information security directors, which allowed to conclude that organizations in Portugal still need to increase their maturity when it comes to information security, and that this may be due to the absence of an established security culture in the country. On the other hand, the CISO's role has been increasing in relevance, being considered that it should have a close and independent relationship with organizations' boards.

Keywords: CISO; Information Security Management; Information Management; Risk Management; Board of Directors

1 INTRODUCTION

Today, information can be seen as a basic need, without which organizations simply cannot operate (Carr, 2003). As we live in an increasingly connected world, information is way more exposed and vulnerable than other types of basic needs (Van Niekerk & Von Solms, 2010).

Organizations are increasingly recognizing information and its related technologies as critical business assets (Cadete, 2015) and, as any strategic asset, it should be effectively managed and safeguarded in order to ensure the success of the business (Doughty, 2003), since an information system incident could cause a business interruption, compromise the organizations reputation and have legal consequences, potentially leading to a financial impact in the organization (Allianz, 2016). For this reason, throughout the years, the approach to information security has been evolving from purely technological to a strategical and business one (Catarino *et al*., 2016).

With the growth of the technology infrastructure, information has also become more vulnerable to a large amount of threats (Olijnyk, 2015). Accordingly, with the 2016 data breach report made by the Identity Theft Resource Center, it has been identified that cyber-attacks have been increasing in frequency and sophistication. In fact, in 2016 a 40% increase of successful attacks has been identified in comparison with the previous year.

Owing to the actual complexity and quick evolution of information security risks, the delegation of a CISO demonstrates the commitment of the organization to the need of a leadership dedicated to answering to business strategic commitments and objectives (Peltier, 2013).

Besides this, recent laws such as the Network and Information Security (NIS) directive and the General Data Protection Regulation (GDPR) have been making organizations rethink their approach and strategy towards information security. Market references such as the COBIT have also been changing their vision of the main functions and responsibilities of the CISO and information security within the organizational context, considering them as a strategic cornerstone in organizations.

The main objective of this work is to understand the current state of information security in organizations and how the recent regulatory changes have been affecting them, understand what the key competences and responsibilities of the CISO are and where should this function be hierarchically positioned in the organizational structure. To accomplish these objectives, an exploratory and transversal study has been performed to understand the events, finding new knowledge and evaluating phenomena from another perspective. For this, interviews were conducted on experienced information security consultants and information systems and information security directors, which allowed to conclude that organizations in Portugal still have a low level of maturity towards information security, and that this may eventually be due to the absence of an established security culture in the country. On the other hand, the recent regulatory changes have been positive to the awareness of the topic in organizations and in the own country, helping increase the relevance of the CISO's role, a general opinion being that they should have a close and independent relationship with organizations' boards. It was possible to conclude that the role and mission of the CISO in organizations can be directly related with the awareness of the matter, allowing to verify that information security is not only an organizational matter, but also a social and cultural one.

2 Literature Review

2.1 The Value of Information

In the organizational context, information is a business enabler. Business processes (supported in information technologies or not) generate and process data that is transformed into information and knowledge, which are used to generate value and drive the organization and their processes (ISACA, 2012).

Information management has been changing the way organizations drive their business and compete with each other, having a key role in empowering their strategic and competitive advantage (Saloojee *et al.*, 2007). Organizations take explicit and implicit decisions about information demand and use. These decisions are based on estimated costs and benefits of the information on their business structure and strategy (Feldman & March, 1981).

Organizations are information consumers, managers and suppliers, being their organizational intelligence reputation built through their capability of assuring, analysing and recovering their information on a timely and efficient way (Feldman & March, 1981).

2.2 Information Security Management

The ISO 27000 standard defines information security as the process of "preserving the confidentiality, integrity and availability of information" (International Organization for Standardization, 2014), being its main mission to ensure business continuity and reducing damage by limiting the impact of information security incidents (Von Solms, 1998). An information security management limited to technologies and information technology processes is not, *per se*, enough to grant a global influence in large organizations (Sajko *et al*., 2011).

Information security governance is defined as the process of defining, establishing and keeping a structure and management processes that support the alignment of information security with business goals and at the same time are consistent with the suitable laws and regulations by adopting policies, controls and establishing roles and responsibilities that support a better risk management in the organization (Bowen *et al.*, 2007). The process of organizing information security in an organization should contemplate factors such as its mission, composition, authorities, responsibilities, roles, lines of communications, coordination and position in the organizational structure (Peltier, 2013).

When defining a guideline for information security management, in 2001 Basie von Solms presented 13 dimensions that, regardless of how they are organized, should work together in order to create a secure environment (Von Solms, 2001): (1) Corporate strategy and governance dimension; (2) Organizational dimension; (3) Policy dimension; (4) Best practices dimension; (5) Ethical dimension; (6) Certification dimension; (7) Legal dimension; (8) Insurance dimension; (9) Human dimension; (10) Awareness dimension; (11) Technical dimension; (12) Metric dimension; and (13) Audit dimension.

Thus, information security should be understood and handled as a multidimensional issue (Von Solms, 2001), and should be addressed as a corporate governance and management responsibility. Risk management, reporting and leadership accountability should be developed in a way to grant an appropriate level of information security maturity on the organization (Posthumus & Von Solms, 2004).

2.3 The CISO's Role

The delegation of a CISO, or someone responsible for information security, shows the need of leadership dedicated to the needs and compromises of information security in any organization (Peltier, 2013). This role can have other names, such as Information Security Director, Information Security Manager or Information Security Officer, but the title is not as important as its responsibilities (Fitzgerald, 2007).

While the CEO and CIO (Chief Information Officer) functions are clearly defined due to the maturity of this roles, the CISO role definition is still in evolution (Fitzgerald, 2007). In the past, their role was mainly focused in defining technical security standards and policies. Today, organizations are becoming aware that cyber-risk is directly related to their innovation and growth strategies (Goodyear *et al*., 2010).

Today, the CISO is becoming more recognised as a core element on the definition of the organization's information risk management strategy (Médice, 2013), having as main responsibilities (SC Jobs, 2017): (1) develop, manage and operationalize the information security strategy; (2) continuously monitor and evaluate the information security practices; (3) perform information security audits and risk assessments; (4) lead, supervise and train its department and team; (4) making the organization compliant with information security regulations; (6) develop and implement business continuity plans; (7) protect the intellectual property of the organization; (8) information security risks and strategy training and awareness of the company's employees; (9) manage information security budgets; and (10) report to the board of directors and being an active member in the top management team.

The CISO has an executive role on the organization and is responsible for establishing and maintaining an organizational information security vision, strategy and program (Goodyear *et al*, 2010) that is consistent with the organization's global strategy (Peltier, 2013).

Although it is possible to conclude that the modern CISO is intrinsically more aligned with the organization's administration and top management than with the technical strand (Cave, 2017), a study performed by ISACA and the RSA Conference with information security managers and professionals verified that 63% of the interviewed still report to the CIO, 14% to the CEO and only 8% report directly to the board of directors (ISACA, 2016).

2.4 Legal and market references changes

ForeScout Technologies' vice president Myles Bray says that regulatory encouragement will help boards of administration reach a higher visibility and security in the organization, its resources and data, stating that this encouragement is a great necessity and positive evolution (Cave, 2017).

It is expected that the adoption of legislation such as the General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) directive have a substantial impact on information security practices in a close future (Brown, 2017), as these legislations create the opportunity for organizations to improve and rethink their information security strategy and structure in order to become a business enabler (Brown, 2017).

One of the most trending recent legal changes in Europe has been the GDPR, which was published by the European Parliament and the Council of the European Union on 27th April 2016 and came into force on May 2018. This piece of legislation has brought specific requirements regarding the rights of the data subject and obligations for the data controllers and processors, bringing penalties for its non-compliance. This regulation states that organizations that process or deal with personal data should implement management and technical measures to ensure the protection of that data. Authorities or public organizations, entities that systematically monitor large amount of personal data or that process high volumes of sensitive personal data should delegate a Data Protection Officer (DPO) responsible for the data protection program in the organization. Entities not covered by the previous types of organizations can also appoint a DPO. The DPO should be independent, report directly to the top management team and should not be dismissed or penalized for performing his duties (Council of the European Union & European Parliament, 2016).

Organizations have been discussing the need of creating a new function for the DPO versus merging it with the CISO functions (Ataya, 2017), as the CISO is responsible for the organization's general information security, which includes the protection of personal data (Approach, 2017). According to the independency requirements defined for the DPO, it cannot be automatically assigned the responsibility to the CISO (Roland, 2017), although companies which are not required to have a DPO should evaluate the need to delegate a person for this charge or allocate the responsibilities to the CISO, ensuring that this merge of functions do not result in a conflict of interests between them. Regardless, the CISO is the best ally for organizations beginning their data privacy program, being responsible for the information risk management, information security incident management and crisis management and has a key role on the definition of the data protection strategic plan (Approach, 2017).

In addition, the NIS Directive has come into force bringing specific measures with the intention of granting a high common level of information and network security in all Europe Union. The main goal of the directive is to increase the robustness of information and network security in the EU, requiring the Member States and their operators of essential services organizations to develop an information security plan and adopting technical and management measures to manage the information and network risks to their operations and services (National Cyber Security Center, 2017; European Parliament and the Council of the European Union, 2016).

The implementation of this directive is reached through the implementation of 14 security principles described in 4 high level objectives (National Cyber Security Center, 2017; European Parliament and the Council of the European Union, 2016): (1) development of appropriate organizational structures, policies and procedures in order to understand, evaluate and continuously manage information and network risks; (2) provide security measures in order to protect the essential services and their systems from cyberattacks; (3) capability to ensure that the security measures remain effective and detect cybersecurity events that impact or could impact essential services; and (4) capability of minimizing the impacts of a security incident on the delivery of essential services.

This directive will help information security professionals to reinforce the importance of information security and encourage a risk management approach on the design of the information security plan (Josi, 2016), empowering the CISO's visibility and communication with the top management team (Augustinos *et al.*, 2016).

In terms of the CISO's exposure to the top management team, the United States of America made an effort by introducing in March 2017 the Cybersecurity Disclosure Act to the USA Senate, with the aim of improving customer protection, increase transparency to investors and grant that information security and data privacy are among the top priorities of public organizations (Homeland Security Today, 2017). This project intended that public organizations reported annually to the SEC (Securities and Exchange Commission) on the knowledge of information security on the boards of directors and, in case there was none, what other information security steps were being adopted to mitigate this lack of knowledge. Many specialists consider that if this directive had been approved it would have represented an extremely positive step in terms of improving the communication and alignment between the information security and business strategies (Ross, 2017).

In terms of market references, COBIT has published in 2012 it's 5th edition providing new recommendations and guidelines about combining business operation goals with IT operation goals and on how to measure these goals. This version provides the professional guide *COBIT 5 for Information Security*, which is focused on a wide number of enablers, such as security functions, titles, committees, processes and policies, providing guidelines for an effective information security management. This guide brings a new vision of the information security strategy endorsed by COBIT. On its previous version, COBIT 4.1 defended that information security should be under the scope of IT management, leaving the information security strategy dependent on the IT strategy (Morimoto, 2009). On the other hand, COBIT 5 defends that the CISO is the responsible for developing an enterprise information security strategy aligned with the business strategy, creating a greater relationship between the CISO and the CIO, CFO and CEO (Wolden *et al.*, 2015).

3 Methodology

3.1 Type of Study

Due to the nature of the investigation and lack of theoretical literature, an inductive approach was conducted in this study, since it's intended to get a deeper understanding of the investigation context and of the individuals related to the context and events. (Saunders *et al.*, 2009).

To reach the investigation goals, an exploratory study was performed to understand the events, to search for new perspectives, and to evaluate the phenomena from another perspective (Robson, 2002, quoted by Saunders *et al.*, 2009). The strategy consisted on a content analysis supported in semi-structured interviews so to collect valid and reliable data relevant to the objectives of the investigation (Saunders *et al.*, 2009). A transversal study was performed in order to understand the current circumstances and gather the opinion of what led to the present state and future predictions.

3.2 Data sampling and collection

The sample is non-probabilistic and self-selected. Since the research is mainly exploratory, the sample was selected with a set of desired characteristics (managers and directors with several years of experience in matters related with information security and information systems, such as CISO's, Information System Managers, Expert Advisors and Auditors).

The sample was obtained through a direct invitation to participate in the interview, and is composed by four CISO's, three CIO's, two expert consultants and one information security technician. This sample was considered sufficient as the opinions by role are strongly consistent, being considered that a saturation point was reached. The sample unfolding is as follows:

CODE	ROLE	INDUSTRY	DURATION	RECORDED
E1	CISO	Energy	~30m	No
E2	CIO and InfoSec Technician	Pharmaceutical	~20m	No
E3	CISO	Banking	~1h10m	Yes
E4	CISO	Regulatory	~35m	Yes
E5	Expert Consultant/Auditor	Audit Services	~55m	Yes
E6	CIO	Pharmaceutical	~25m	Yes
E7	Expert Consultant	Consulting Services	~45m	Yes
E8	CISO	Research and Consulting	~1h15m	Yes
E9	CIO	Law	~50m	Yes

Table I – Interviewees List

All interviews were performed throughout 2018 and, apart from the interview with E2 which was performed by phone, were all conducted face-to-face. Interviews were semi-structured so to collect qualitative data by exploring the interviewee's speech.

3.3 Data analysis

According to Bardin (2010), content analysis consists on a set of techniques of analysis of communications to obtain systematic and objective perspectives that allow to infer knowledge related to these messages.

To perform this analysis, the following actions are required (Vala, 1986): (1) delimitation of the goals and definition of a theoretical framework to guide the research; (2) constitution of a corpus; (3) definition of the categories; (4) definition of units of analysis; and (5) quantification.

Considering that all the material for the analysis was obtained through interviews, the analysis corpus is composed by all the information collected, being that the categorization aims to reduce the complexity of the material to be analysed, organizing it to enhance the apprehension and explanation of the information to be retained (Vala, 1986).

In order to perform this analysis, the content of the interviews was transcribed by units of analysis. No software was used to analyse this data.

4 RESULTS

4.1 General Information Security Environment

In order to understand how the vision and awareness of information security has evolved over time, the initial part of the interviews attempted to obtain an understanding of the general context, evolution and future perspectives regarding the information security environment in the respondents' organizations. It was possible to verify that the role of information security in organizations was initially very technical (E1, E3, E4 and E7), although there are still several organizations that focus mainly on the technical security aspect (E2, E6 and E7) and that the CISO (or the person responsible for security issues) is not fully allocated to respond to these issues (E5). Particularly, it has been found that the security budget in most respondents' organizations of is defined by the IT (E1, E2, E6 and E9), and only CISOs E3 and E4 claim to have their own budget.

Although there is still a strong focus by organizations on the technical side of security, E7 and E8 agree that there is an increasing awareness that protecting the security perimeter is not enough. Even with this paradigm shift, there is the view that organizations in Portugal still have a very reduced and mostly reactive security maturity (E2, E5, E7 and E9), although some organizations are already adopting a more preventive strategy (E1 and E5), including contracting external security event monitoring and detection services, so that they may be more focused on defining a security strategy (E6) and investing in information security incident insurances in order to be financially safeguarded from a disruptive incident (E1 and E6).

It was possible to verify an interest in investing in security intelligence and intelligence gathering (E1 and E5) in order to make security smarter and less intrusive (both for business and people) (E1). However, E5 claims that work in this area is still far behind. E7 and E8 argue that there is a cultural problem in Portugal regarding information security, which is a major obstacle to the maturity of the topic in the country. There is, however, the view that recent regulatory changes, both internal (imposed by national regulators) and external (such as NIS and the GDPR), are changing culture and awareness for security issues in the country (E1, E2, E5, E7 and E8).

4.2 CISO profile and responsibilities

Although it has become clear that security is becoming more and more detached from a purely technical aspect, there is a general view that the CISO, although not needing to be a pure technician, must also have a technical background (E1, E3, E4, E5, E7 and E9), since they should have a critical view on information security issues (E1), be aware of existing techniques (E4), and be able to communicate adequately with the technical teams responsible for the topic (E5 and E7). In addition, the CISO should also have a business (E3, E4, E7), governance (E5, E7) and strategic vision on security issues (E1, E7 and E8).

E1 believes that CISO should be a leader, being able to manage people and have good communication skills, both up and down on the organizational chain (E1, E3, E4 and E6), and should also have a reporting capability to appropriately pass the message to the board (E1, E3 and E5). To be able to transmit the message properly, the CISO must be able to communicate how the security risks which the organization is exposed may manifest in risks to the operation of the organization and must be able to understand and transmit not only in terms of financial risks, but also social and environmental risks (E1 and E3). E3 and E5 state that for this, the CISO should have a close business relationship and not have a purely IT-focused security vision, must understand all existing information assets, and how these are related to the daily operation of the different areas of the organization. However, the CISO should also be very close to the IT activities, being considered by E4, E5 and E8 that if there is security monitoring throughout the information systems project development process, costs can be reduced in future corrective interventions, since this monitoring contributes to the greater robustness of the systems in terms of security since its conception.

The CISO must also have a strong critical sense, must be able to deal with pressure in order to take calculated risks (E3), and should be focused on the continuous improvement of their activities and areas of responsibility (E3, E4 and E8).

Analysing the areas of intervention under the CISO's responsibility, it was possible to identify 8 main areas, namely: (1) training and raising awareness of employees and stakeholders (E1, E5, E6, E7, E8 and E9); (2) risk management (E1, E4, E5, E7 and E8); (3) business continuity management (E1, E3, E4, E7 and E9); (4) incident management (E4, E5, E8 and E9); (5) definition of a governance model, policies, processes and procedures (E1, E5, E7 and E8); (6) audit (E1, E3 and E9); (7) compliance with good practices and regulations (E4 and E8); and (8) identity and access management (E1 and E2).

In performing their tasks, some challenges have been identified that impact the strategy and operation of the information security management system, namely: (1) obtaining investments in an area that does not have direct financial returns (E4, E5, E6, E7 and E9); (2) aligning people with the security strategy (E1, E5, E7, E8 and E9); (3) communicating effectively to management (E1, E4, E5 and E9); (4) the impact of information security controls on people (E1, E3, E5 and E9); (5) aligning security with the organizational context (E3, E5, E8 and E9); (6) the impact of security and controls on daily operation in the organization (E1, E6 and E8); (7) investment in people (E4 and E7); and (8) resistance to change (E3 and E9).

4.3 Impact of regulatory changes

There was a general alignment regarding the positive impact of the GDPR on organizations, in particular by raising awareness of security issues (E1, E2, E7 and E8) and improving security in the organizations (E1, E2, E4 and E5). It was stated by E8 that the board’s legal accountability for this matter has been a great contribution empowering an information security culture and awareness in organizations. By the other hand, E7 and E9 consider that the lack of compromise by the Portuguese State regarding to the Regulation became an obstacle for the organizations’ commitment with its goals, reducing the potential increase of information security culture in the country.

Regarding the profile of the DPO, it was verified that most of the organizations of the interviewees that delegated a DPO, chose a legal profile (E1, E4, E7 and E9), with only E3’s organization delegating someone from the information security area. Regardless of the background of the DPO, there is a vision that, for the Regulation to be successfully implemented, there must be a joint work between security and legal (E1, E3, E4 and E7).

It has been identified a much lower awareness of the NIS Directive. E5 argues that the Directive has been stifled by the Regulation and E8 believes that this can also be justified by the fact that it is targeted only at essential service providers and has a much less widespread impact on society. Although its scope is more reduced than the GDPR’s, it is considered by E8 that, since most organizations under the Directive’s scope are partially controlled by the Portuguese State, that this could increase the Portuguese Government's awareness and help spreading an information security culture through the country. It is argued by E7 and E8 that in terms of security the Directive is much more urgent than the Regulation.

E5, E7 and E8 stated that for these regulatory changes to be taken with due seriousness and commitment, as well as with a perspective of continuous improvement, there must be a greater regulatory inspection than the one existing to date.

4.4 Hierarchical structure and reporting lines

Regarding the hierarchical positioning of security in the organization, it was found that due to the need to align security with the organization's strategy and to transmit information security risks and their impact to management, there is an alignment with the need for CISO to directly report to the board (E1, E3, E4, E5 and E8) and to be independent (E3 and E4). Consultants E5 and E7 go even further by arguing that CISO should even be part of the board itself, derived from the criticality of their function for business strategy.

Since information system risks are always at the top of the organization's risk chain (E4 and E6), and because it is a much more risk-oriented function than technological (E8), so that there are no conflicts of interest, the security officer should not be below or report directly to the IT director (E3, E4, E5, E7 and E8).

E3 and E4 clearly argue that the CISO cannot be at the bottom of the hierarchical chain of organizations, since the lower in the pyramid this function is, the more susceptible it is to conflicts of interest and to withdrawing strength from the CISO next to the board.

When addressing the issue of the Cybersecurity Disclosure Act of 2017 and its goal of ensuring that boards have knowledge of the issues and risks of information security, the overall opinion was positive (E1, E3, E4, E5 and E7), and it was considered that a similar measure should also be applied in Portugal or in Europe (E1, E3, E4 and E7). Despite the positive impact this measure can bring, the concern is that organizations follow this measure only from the point of view of compliance (E5 and E7). However, it was possible to verify that some work already exists in this direction in Portugal.

5 DISCUSSION

The analysis allowed to verify that, although this is changing, organizations in Portugal are still very focused in a technical and reactive view of security, with no strong connection to the business and not being considered as a strategic topic.

Comparing these results with existing literature, it is possible to verify that there is a delay in security's maturity in Portugal, since most of the theory points out the need of top management commitment to the information security management system.

However, while there were still several cases where information security was placed under IT, there begins to exist an alignment, as argued by Sajko *et al* (2011), regarding this being an insufficient approach to ensure a global and appropriate influence in the organization.

Fitzgerald (2007) argued that, unlike other C-levels, the CISO's role was still being defined and evolving. This was also verified, which can be justified by the existing lack of maturity in Portugal regarding this topic. This lack of commitment seems to mainly have a cultural origin, feeding the vision that information security crimes are a topic that neither affects nor has a great impact in Portugal due to the country's reduced geographic and geopolitical exposure.

It was, however, possible to verify that the security environment in organizations has been changing and evolving. This change has come a long way, according to Brown's (2017) expectations regarding the impact of the recent legislative changes and the cultural change that they have brought. Despite a low state commitment to regulatory changes from the EU, there has nevertheless been a cultural shift in relation to security issues. It is considered that what currently exists is still not enough, but it is a start. It is expected that directives such as NIS (which directly impact the State) and internal regulatory changes can contribute to deepen the culture and maturity of security in Portugal.

According to Peltier (2013), larger organizations should consider the need to have a CISO independent of organizational elements. Of the interviews conducted, there were only two cases in which this independence existed, although in one case independence was lost. Due to the GDPR's imposition that the DPO be an independent person within the organization, and the possibility of this responsibility being assumed by someone from security, there was an expectation that this requirement would bring more independence to the role of security in organizations. However, from the interviews, it was found that the Regulation was not a great contribution in this sense, since the only case in which responsibility was assigned to a security person, an independent CISO already existed.

Regarding the CISO's profile and responsibilities, there was a general alignment between the interviewees and the theories by Cave (2017), Peltier (2013) and Fitzgerald (2007) namely: (1) about the need for the CISO to have experience in risk and security management positions, and to also have technical knowledge (Cave, 2017); (2) about the need for the CISO to be a leader with a strategic vision (Peltier, 2013); (3) about the need to be focused on the organization's strategy (Cave, 2017); (4) that security should not be at the bottom of the organizational hierarchy (Peltier, 2013); (5) that the CISO should have a close interaction with the administrative councils (Peltier, 2013); (6) that the CISO should be independent (Peltier, 2013); and (7) the need for the CISO to have the responsibility of establishing a security culture in the organization (Fitzgerald, 2007)

There was also an alignment with the 13 dimensions for information security management presented by von Solms (2001), although the ethical dimension was not addressed. Regarding the responsibilities of the CISO presented by SC Jobs (2017), it was not possible to identify organizations that had the CISO incorporated in the top management teams, and in organizations where security is below the IT dimension, the budget dimension ends up not being their responsibility. Only the expert consultants shared the view that the CISO should have a position on the board of directors, and it was not possible to verify this reality in any of the organizations of the interviewees. It was also possible to gather the main challenges for the correct performance of their functions, in addition to the challenge of aligning people with the security program, besides other challenges such as obtaining financing to invest in security, in effective communication to management, in the direct impact that security has on people and in business operations, and in enabling security in the organizational context. However, it is the CISO's responsibility to influence and improve organizational culture in order to support information security.

Regarding the position of the CISO within the hierarchical structure of the organization, there were several cases where security was under the control of the Direction of Information Systems (DSI), contrary to what Peltier (2013) defended, as well as some of the interviewees. Respondents who opposed the allocation of security below IT argue that this decision compromises the independence of the security function, since information technology and security have competing interests.

Although it was not possible to conclude on the need for CISO to belong to the boards of directors, as defended by SC Jobs (2017), it was possible to understand the need for security matters to arrive to the top management without any filters and the need for a close relationship between the CISO and the boards of directors. The fact that it is not possible to draw a solid conclusion on the need for the head of information security to belong to the boards of directors could be directly related to the lack of maturity and culture for the subject in Portugal.

6 Conclusions

This study presents an overview of the current state of information security maturity in Portugal, as well as the course that is being followed. It is possible to conclude that this maturity in the country is still reduced compared to the expected and desired.

A positive impact of the regulatory changes on information security awareness in organizations and in the country has been verified. The privacy requirements imposed by the GDPR is leading to a cultural change and there is hope that the implementation of the NIS directive will empower information security awareness, mainly to the Portuguese State, which will be strongly affected by this directive.

It was possible to identify a relationship between the CISO role in organizations and the awareness that exists for the subject of security within them. In organizations where there is less maturity for security issues, the person in charge of this area is typically under the IT department. In organizations where boards of directors are more aware of information security risks and their impact on business operations, organizational strategy, and reputation, the CISO has a greater proximity and independence with them.

Although the expert consultants believe that it makes sense for the CISO to have a close relationship with the board of directors, this vision is not yet verified in organizations in Portugal.

It can be concluded that the CISO role and their mission in organizations may be directly related to the awareness that exists on the matter, and that information security is not only an organizational matter but also a social and cultural theme.

Some research limitations were identified, such as the fact of being a transversal study, gathering information at a single point of time, not allowing a deep perception of the evolution of the study matters as a longitudinal study would allow. The fact that the data collection was gathered through semi-structured interviews is also subject of limitations inherent to the technic itself, such as misunderstanding of the questions, inconsistent answers and inability to answer to the interviewer questions.

Relating to future research, some opportunities were identified, such as performing a longitudinal study with a wider scope (in terms of business sectors, roles and geographies). It is also recommended the execution of a transversal study in order to understand how the information security culture in a country affects information security maturity and awareness in its organizations and citizens.

ACKNOWLEDGEMENTS

We are gratefully acknowledge financial support from FCT- Fundação para a Ciencia e Tecnologia (Portugal), national funding through research grant UID/SOC/04521/2019.

REFERENCES

Allianz (2016). *Allianz Risk Barometer - Top Business Risks 2016*. Consulted in 9th October 2017. Available in http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf

Approach (2017). *Why do you need a CISO?*. Consulted in 18th March 2018. Available in https://www.approach.be/en/images/gdpr_-_why_you_need_a_ciso-short.pdf

Ataya, G. (2017). *Can a CISO act as a DPO?*. Consulted in 18th March 2018. Available in https://www.linkedin.com/pulse/can-ciso-act-dpo-georges-ataya/

Augustinos, T. P., Bauer, L., Cappelletti, A., Chaudhery, J., Goddijn, I., Heslault, L., ... & Leverett, E. (2016). *Cyber Insurance: recent advances, good practices & challenges*.

Bardin, L. (2010). Análise de conteúdo.(1977). *Lisbon (Portugal): Edições*, *70*, 225.

Bowen, P., Hash, J., & Wilson, M. (2007). Information security handbook: a guide for managers. In *NIST SPECIAL PUBLICATION 800-100, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*.

Brown, D. (2017). *Is New Regulation a Threat or an Opportunity for Security Strategy?*. Consulted in 18th March 2018. Available in https://www.fireeye.com/blog/executive-perspective/2017/05/new-regulation-security-strategy.html

Cadete, G. (2015). Using Enterprise Architecture for COBIT 5 Process Assessment and Process Improvement. *IST, Portugal*.

Carr, N. G. (2003). IT doesn't matter. *Educause Review*, *38*, 24-38.

Catarino, T. M., Vasconcelos, A., & da Silva, M. M. (2016). The Role of the Chief Information Security Officer. *IST, Portugal*.

Cave, K. (2017). *Does the CISO role need to be formalised?*. Consulted in 18th March 2018. Available in https://www.nacdonline.org/AboutUs/NACDInTheNews.cfm?ItemNumber=40736

Regulation, P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *REGULATION (EU)*, 679.

Doughty, K. (2003). Implementing enterprise security: a case study. *Computers & Security, 22(2)*, 99-114.

Feldman, M. S., & March, J. G. (1981). Information in organizations as signal and symbol. *Administrative science quarterly, 26(2),* 171-186.

Fitzgerald, T. (2007). Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other. *Information Systems Security, 16*(5), 257-263.

Goodyear, M., Goerdel, H., Portillo, S., & Williams, L. (2010). Cybersecurity management in the states: The emerging role of chief information security officers. *Available at SSRN 2187412*.

Homeland Security Today (2017). *Oversight Transparency of Cyber Risks at Publicly Traded Companies Addressed in New Bill*. Consulted in 18th March 2018. Available in https://www.hstoday.us/channels/global/oversight-transparency-of-cyber-risks-at-publicly-traded-companies-addressed-in-new-bill/

ISACA. (2016). *State of Cibersecurity Implications for 2016: An ISACA and RSA Conference Survey*. Consulted in 18th March 2018. Available in http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

ISACA. (2012). *COBIT 5: Modelo Corporativo para Governança e Gestão de TI da Organização*. Rolling Meadows: ISACA.

International Organization for Standardization. (2014). *ISO/IEC 27001: 2014*: *Information security management systems - Overview and vocabulary*. International Organization for Standardization.

Josi, M. (2016). *What does the new EU Network Information Security Directive imply?*. Consulted in 18th March 2018. Available in https://www.cyan.network/news/what-does-the-new-eu-information-security-directive-implies

Médice, R. (2013). *O Papel do Security Officer (Agente de Segurança)*. Consulted in 18th March 2018. Available in https://www.profissionaisti.com.br/2013/07/o-papel-do-security-officer-agente-de-seguranca/

Morimoto, S. (2009). Application of COBIT to security management in information systems development. In *2009 Fourth International Conference on Frontier of Computer Science and Technology* (pp. 625-630). IEEE.

National Cyber Security Center (2017). *Networks and Information Systems (NIS) Directive: Security objectives and principles*. National Cyber Security Center

Olijnyk, N. V. (2015). A quantitative examination of the intellectual profile and evolution of information security from 1965 to 2015. *Scientometrics*, *105(2)*, 883-904.

Peltier, T. R. (2013). *Information security fundamentals*. CRC press.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & security*, *23*(8), 638-646.

Roland, N. (2017). *Would my CISO be my DPO? Information Technology Privacy*. Consulted in 18th March 2018. Available in https://commyounity1.wordpress.com/2017/06/23/would-my-ciso-be-my-dpo/

Ross, A. (2017). *What is the Cybersecurity Disclosure Act of 2017?*. Consulted in 18th March 2018. Available in https://baydynamics.com/blog/video-cybersecurity-disclosure-act-2017/

Sajko, M., Hadjina, N., & Sedinić, I. (2011). Information security governance and how to accomplish it. *MIPRO, 2011 Proceedings of the 34th International Convention*. IEEE.

Saloojee, R., Groenewald, D., & Du Toit, A. S. A. (2007). Investigating the business value of information management. *SA Journal of Information Management, 9(1).*

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students 5th ed. *England: Pearson Education Limited*.

SC Jobs (2017). *Job Description: Chief information security officer*. Consulted in 18th March 2018. Available in https://www.scmagazineuk.com/job-description-chief-information-security-officer/article/629762/

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & security*, *29*(4), 476-486.

Vala, J. (1986). A análise de conteúdo. *In A. S. Silva, & J. M. Pinto, Metodologia das Ciências Sociais* (pp. 101-128). Porto: Edições Afrontamento

Von Solms, B. (2001). Information security—a multidimensional discipline. *Computers & Security*, *20*(6), 504-508.

Von Solms, R. (1998). Information security management (3): the code of practice for information security management (BS 7799). *Information Management & Computer Security*, *6*(5), 224-225.

Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System. *IFAC-PapersOnLine*, *48*(3), 1846-1852.