NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação

Master Program in Information Management

How Cyber Governance Influences Relationships Between Companies

Sérgio Luís De Matos Rodrigues Ribeiro

Dissertation presented as the partial requirement for obtaining a Master's degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

How Cyber governance Influences Relationships between companies

Sérgio Luís de Matos Rodrigues Ribeiro

Dissertation presented as the partial requirement for obtaining a Master's degree in Information Management, Specialization in Information Systems and Technologies Management

Advisor / Co-supervisor: Andrew C. E. Harcourt

September 2019

Declaration of Originality

I declare that the work described in this document is my own and not from someone else. All the assistance I have received from other people is duly acknowledged, and all the sources (published or not published) are referenced. This work has not been previously evaluated or submitted to NOVA Information Management School or elsewhere.

Lisboa, 19 September 2019, Sérgio Ribeiro

[the signed original has been archived by the NOVA IMS services]

Acknowledgements

I would first like to thank my thesis advisor Mr. Andrew C.E Harcourt of the Nova IMS University. The door to Prof. [Harcourt] office was always open whenever I ran into a trouble spot or had a question about my research or writing. He consistently allowed this paper to be my own work but steered me in the right the direction whenever he thought I needed it.

I would also like to thank the experts who were involved in the validation survey for this research project. Without their passionate participation and input, the validation survey could not have been successfully conducted.

Finally, I must express my very profound gratitude to my parents and friends for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Author
Sérgio Ribeiro

Abstract

The growing complexity, variety and sheer volume of cyber-attacks have proven companies are facing a significant level of pressure from both internal and external threats. These, impact on their daily operation and, consequently, on the market perception of their various stakeholders.

For companies to fight these threats and keep their data protected, the need to implement a robust security framework is gaining more importance. What is also clear is that companies can no longer rely solely on technological tools to keep data safe and secure.

This study focuses on how the relationships between a company's business and its partners (customers, suppliers, etc.) are affected by the cyber governance strategies. Furter an understanding of the organization's culture of governance and security implemented within

The article analysis suggests that although cyber governance plays a crucial role in business these days, companies appear to find it challenging to identify the best policies and strategies to implement both internally and also with their corporate partners.

Keywords

Cyber-attacks, Cyber Governance, Policies, Threats, Interorganizational Networks, Procedures.

Acronyms

AI - Artificial Intelligence

CAIQ - Consensus Assessments Initiative Questionnaire

CISM – Certified Information Security Manager

CISO – Chief Information Security Officer

CISSP - Certified Information Systems Security Professional

CRISC – Certified in Risk and Information Systems Control

CSM – Cyber Security Manager

CSO – Chief Security Officer

DB – DataBase

DoS – Denial of Service

DPO – Data Protection Officer

EU – European Union

GDPR – General Data Protection Regulation

IaaS – Infrastructure as a Service

IoT - Internet of things

IS – Information Security

ISO – International Organization for Standardization

IT – Information technology

ITIL - Information Technology Infrastructure Library

NDA – Non-Disclosure Agreements

Paas – Product as a Service

SaaS – Software as a Service

SDLC - Software Development Life Cycle

SOC – Systems and Organizations Control

SSAE - Statement on Standards for Attestation Engagements

SSCP – Systems Security Certified Practitioner

INDEX

1. Introduction

As cybercrimes have been experiencing a sturdy increase over the past years, cybersecurity is gaining more and more relevance not only in the private sector but also in the public sector. Research also shows an increase in the number of connected IoT devices; even the volume of information generated is increasing.

The sharp and sustained increase in the amount of information produced within organizations has compelled companies to make substantial investments to protect their assets successfully and to ensure cyberattacks are highly prevented at a corporate level. For this reason, cybersecurity plays a significant role in companies nowadays

As more and more businesses are getting attacked and the individuals responsible for those attacks become more knowledgeable about cybersecurity, companies' urge to develop and implement a successful cyber governance framework as high as the need for them to keep an eye on effective ways to overcome those threats. As a consequence, cybersecurity is, more than ever before, a hot topic at corporate board meetings

The current technology evolution has consequently triggered the evolution of cyber-attacks. This evolution resulted in the existence and frequent occurrence of viruses, e-mail spam, Trojan horses, spyware and ransomware' that affect not only personal but also enterprise infrastructures causing a significant amount of financial losses and productivity issues (Bagchi & Udo, 2003).
For example, “the average cost of a data breach ranges from $2.2 million for incidents with fewer than 10,000 compromised records” (“Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT,” 2018). At the end of 2017, hundreds of millions of persons were affected by the Equifax data breach. The cost from the data breach ended with a settlement of $700 million which led to approximately 4$ (“Equifax owes you a lot more, but here’s how to get $125 from this week’s settlement—The Verge,” n.d.). Of that, Reuters said, “$125 million will be covered by an insurance policy”. (“Equifax breach could be most costly in corporate history,” 2018)

Companies that agree to form partnerships in terms of data sharing might have higher returns in spite those who refuse to cooperate between each other; however, this can also put them at risk (Harcourt, 2018).

All in all, these corporate partnerships represent cooperation between businesses and competitive advantage these returns result in collaboration and competitive advantage to the

market. These Interorganizational networks are nowadays stronger this was because of the growth of SaaS solutions that have allowed a higher multi-directional data integrations between organizations. Previously the main focus of these cooperations' has been "Easy integration" within minimal concern for data security; yet the bond between them can be highly prejudicial to one or another (Baker & Faulkner, 2017; Gnyawali & Madhavan, 2001).

The uprising number of cyber-attacks and companies affected have brought the subject of cybersecurity to another level. Further, regulations like the GDPR have brought to the table areas like law to the public, where the need to be compliant and to assure data privacy is more than ever a directive ("European Commission—PRESS RELEASES - Press release—General Data Protection Regulation shows results, but work needs to continue," n.d.). After all, it may not only be a particular company that experiences cybersecurity threats, but also one of its partners with whom they have a partnership. Hence, the urge to fully understand how cybersecurity measures, strategies and frameworks implemented at a corporate level impact these inter-organizational networks.

This study seeks to contribute to the comprehension of these interrelations, through the research of the cybersecurity subject combined with the understanding of the individual's actions and their expertise in the area to adopt or implement rules and processes within their companies. The best way to get this perception is by understanding the companies' business operations and procedures by gathering specific cybersecurity information from the individuals responsible for the implementation of these measures, strategies and frameworks.

Therefore, this paper focuses on the following questions: Firstly, verifying whether companies have cyber governance policies and processes regarding their partners?; Secondly, validating if the people who are in charge of securing the companies' data are certified to undertake that responsibility successfully?; Thirdly, understanding the different types of policies and processes that are put into practice and how often these companies conduct a fully detailed review/audit of them to ensure they are always be updated and secured;

By doing so, the most common measures that are believed to keep a company's data secured will be highlighted. Finally, presenting a suggestion of a possible framework of basic actions to help build, engage and protect the relationships between companies.

The framework will serve as a base from where companies should make their starting point to ensure data protection is taken seriously and at a high level of security. Hence, this paper intends to bring awareness around the cybersecurity theme on inter-organizational

networks and to be a reference point for future researches. To help in this study, a questionnaire of 116 professionals of cybersecurity from different sectors and countries was conducted. Here the geographical localization is not a significant factor to be studied; however, for future reaches a more specific understanding between more developed countries would be more beneficial to help improve the framework.

The remainder of the paper is structured as follows. On the second section, a theoretical background supported with a literature review regarding cybersecurity and inter-organizational networks. On the third section, a conceptual model of a framework using key policies and processes. On the fourth section, a detailed analysis of the data collected using quantitative methods as also an understanding of the answers regarding more specific questions. Here, the geographical localization is not a significant factor to be studied; however, for future reaches a more particular understanding between more developed countries would be more beneficial to help improve the framework;

On the fifth section, the discussion of findings and results and to finalize the sixth section the presentation of the conclusions and key takeaways.

2. Theoretical Background

Cyber-attacks have become a day to day occurrence, and the office of the CISO as an area is becoming a sector with higher visibility and importance these days, as opposed to the previous decade where only some companies had only one single professional dedicated to the cybersecurity area and in some cases, some of them dedicated less than 9 hours to it (Hoffer and Straub 1989). The changes that technology experienced has made this sector suffer changes in a way that the health of a company now relies on how well rules and policies are implemented (Poppensieker & Riemenschnitter, 2018). When exploring the study field of cybersecurity we find ourselves concerned about the human factor and in seek of ways to deterring the incorrect behaviours by the way punishment or reward (Chen, Ramamurthy, & Wen, 2012) as well the compliance with the IS security policies in their organizations (Siponen & Vance, 2010). In the previous days talking about cybersecurity was talking about methods to assure the data security and integrity over their networks (Boockholdt, 1989).

Studies conducted before the new millennium show concern regarding the security of information systems, data integrity, computer abuses and how to discipline the perpetrators (Boockholdt, 1989; Jr. Straub Detmar W. & Nance, 1990).

Previously data security was wholly physical. Then when cybersecurity became a priority, the focus was solely on using technology to mitigate risk. However, the focus changed, and companies start addressing human risk via policy & process (D. W. Straub & Welke, 1998).

According to Smith, Milberg, and Burke (1996), "it has become apparent that organizational practices, individuals' perceptions of these practices, and societal responses are inextricably linked in many ways". These practices should come from the managers that cope with the information systems, they are the ones with the ability to inform and help their companies to have more secure policies; however, they not always realize the risks that exist and fail in the implementation of frameworks or models (D. W. Straub & Welke, 1998). These should be informed of the various forms of attack such as DoS, worms and viruses, Spam via email, trojan horses that can affect their personal computers which can compromise their IT infrastructure as well as their companies which can cause significant problems at the operational level but mostly at the financial level (Bagchi & Udo, 2003; Stafford & Urbaczewski, 2004). Despite the use of theories such as the deterrence theory, the neutralization theory, the compliance theory or control theory to understand and help to improve the misuse of information systems (Chen et al., 2012; Siponen & Vance, 2010), none of these theories was put in practice so many time as the deterrence theory, where managers would identify what were the proper and improper ways to use the information systems and implement policies to help deterrent the bad uses of the information system (Straub Jr., 1990).

However, in the new millennium, and according to Gartner, Inc's forecast. "8.4 billion connected things will be in use worldwide in 2017, up 31 per cent from 2016, and will reach 20.4 billion by 2020". With this current growth of the number of IoT devices, managers have a massive sense of responsibility and a high level of pressure on them to be in control of the human factor. Many researchers try to extend the study to the psychological side of human behaviour (H. Liang & Xue, 2009). This study is extended not only to the people that work directly with technology but also the ones that are responsible for the attacks, regardless of them being insiders or outsiders of the company (N. (Peter) Liang, Biros, & Luse, 2016).

This comprehension involves the understanding of how users engage with the information systems and what daily processes are undertaken and taken into consideration according to their roles and responsibilities (Boyce et al., 2011).

Thus, one factor that is of a great deal to better understand this engagement is their motivation, more precisely the motivation to perform secure behaviours. Just like (Menard, Bott, & Crossler, 2017) concluded in their study regarding users motivation in contributing for better information security, "Understanding end-users' motivation to perform secure behaviours will lead to practices driving greater adoption of secure countermeasures and will contribute to an overall safer computing environment ". Nevertheless, motivation can be a good factor in the insider or can become a bad factor in security processes (Posey, Roberts, & Lowry, 2015). Employees with a lack of motivation or negative aspirations can become liabilities - these are considered as insiders. This lack of motivation comes from the unhappiness of the insiders with their companies, also known as "work-related grievance" (Willison & Warkentin, 2013). As we can see, all the cybersecurity theme revolves around user usage and their behaviour with technology that relates to the types of attacks. Authors like Chatterjee, Sarker, & Valacich, 2015 studied the behaviour of the roots that lead to the user misusage; however, because it is a theme that might enter into the psychology field and the way to explain was by linking the behaviour with incorrect practices of the users.

When trying to extend the research of cybersecurity to the inter-organizational networks, we find that there is a lack of comprehension of how secure they are and how best to govern them. However, more and more companies are relying on these cooperations', although these can only happen when companies understand what their needs and position in the market are and how this interorganizational network would come as an advantage (Håkansson & Ford, 2002). The expansion of the internet was one of the significant factors that unlocked the threat vectors, helping to have bigger and better networks by enabling efficient cooperation and lowering costs on processes and other assets (Afuah, 2003). These relations are called "relational pluralism" - the better this relation, the higher the outcome with flexible networks, stable relationships and the ability to adopt tailored innovations (Shipilov, Gulati, Kilduff, Stan Li, & Wenpin Tsai, 2015). According to (Majchrzak & Jarvenpaa, 2010), these relations are only effective being in a safe context, and the managers within collaboration understand what is perceived as a successful collaboration. These factors are the electronic means by which the information is shared between collaborative companies and the geographic

proximity of the collaborators in their network. Within this context, we can understand how these inter-organizational networks help in the comprehension and prevention of IT changes. While the exchange of information between the inter-organizational networks is a high success factor in terms of health, we find that these also become a challenge to the information security control around managers (Anderson, Baskerville, & Kaul, 2017). The transformations occurring cannot and should not be handled by one single manager in a company but by opening boarders discussing the transformations and understanding the changes with other managers within the inter-organizational network. With this approach, managers and policymakers makers are able to adapt their environment to different types of changes in a much better and accurate way (Lucas Jr., Agarwal, Clemons, El Sawy, & Weber, 2013). Recent studies regarding the impact of having a C-level manager helping and backing up the lower managers responsible for the cybersecurity operations showed that companies that have the culture of having a more supported IT area have a more significant wealth effect - this means that when cybersecurity is held by different managers that communicate and are aligned with objectives, the turnover is higher (Benaroch & Chernobai, 2017). Although, managers and policymakers try to put into place the best rules and policies to make their culture inside their companies to raise awareness, the process will not be successful if the employees do not understand the threat that is at stake and if the culture that exists is an ignoring culture or even a blame culture (Spears & Barki, 2010).

The understanding by the employees would help in the task of securing information and having more information privacy. Consequently, this would also help the IS managers in their mission of changing or adapting the current policies whenever needed because only with the daily routines and challenges can they understand and get a grasp of what is wrong and what can be improved (Smith, Milberg, & Burke, 1996).

3. Conceptual model

To help understand the inter-organizational networks relations and the different procedures within each company, several questions were made.

The questions enquired were based on a set of different papers and researches, and the final result was a survey (Table 1) with both quantitative and qualitative questions. Considering

that it is not possible to adapt one specific model of analysis to respond to all enquiries, the final outcome will be based on the survey's answers and standard practices.

Table 1

Question	**Reference**
What is your company size?	(Afuah, 2003)
In which sector is your company?	(Afuah, 2003)
In which area of your company do you Work?	(Afuah, 2003)
Does your company have Processes and Policies relating cybersecurity?	(Dey, Lahiri, & Zhang, 2012; Hui, Kim, & Wang, 2017; Zviran & Haga, 1999)
Has your company ever been the victim of a cyber-attack?	(Dey et al., 2012; Gordon, Loeb, & Sohail, 2010; Hui et al., 2017)
Does your organization conduct System Acquisition, Development and Maintenance?	(Galbreth & Shor, 2010; Wolff, 2016)
Does your organization have Policies and Processes in place to control government changes to all aspects of your IT infrastructure?	(Benaroch & Chernobai, 2017; Lee, Ahn, & Bang, 2011)
Does your organization outsource software development and Hardware acquisition?	(Wolff, 2016)
Does Your organization require suppliers to adhere to an Information Security policy as part of supplier relationships?	(Zhao, Xue, & Whinston, 2013)
Does your organization contract with third-party service providers and if so, how regularly are contractor services monitored, reviewed, and audits are carried out?	(Kumar, Park, & Subramaniam, 2008; Zhao et al., 2013)
Do information security considerations form part of your overall sourcing and supplier management activities?	(Benaroch & Chernobai, 2017; Galbreth & Shor, 2010; Wolff, 2016)
Does your organization outsource to any third-party vendors who will have access to sensitive or critical assets or data (e.g. back up vendors, service providers, equipment support vendors, etc.)	(Zhao et al., 2013)
Does your organization have policies and processes to identify and respond to changes to supplier services?	(Benaroch & Chernobai, 2017)
Does your organization communicate Information Security policies and procedures to Employees, Contractors, Customers and Suppliers, and how is it communicated?	(Siponen & Vance, 2010)
In your company is there a specific person with responsibility for ensuring that rules	(Benaroch & Chernobai, 2017)

regarding third-party suppliers are adhered to and is it a requirement for that person to have any kind of training or certification (e.g. ISO)?	
If your organization has target systems that reside in a data centre, what kind of standards do you ask for? (somebody else's data centre)	(Galbreth & Shor, 2010; Wolff, 2016)
What evaluations do you do demand in case of trying to buy hardware/software from a third party?	(Galbreth & Shor, 2010; Wolff, 2016)

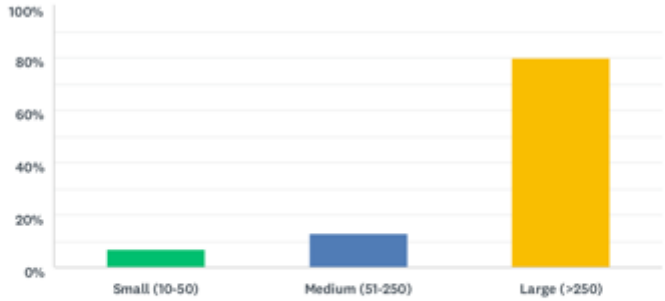
4. Data Analysis and Results

4.1. Data Normalization

In order to have a better analysis of the data acquired, normalization was performed. In this normalization the Question 10 which is "Does your organization contract with third-party service providers and, if so, how regularly are contractor services monitored, reviewed, and audits carried out?" was spilt in two questions to one where we understand which companies contract with third-party service providers and If they do how often are the contracts monitored. The IP addresses were transformed in locations to have new information from the respondents, which is Country. In the Sectors and Area questions, names that meant the same were modified in only one unique name so that the answers could show more detail.

4.2. Question Analysis

- Question 1: What is your company size?

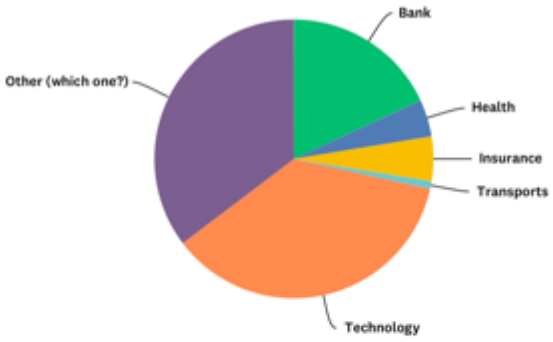


ANSWER CHOICES	RESPONSES	
Small (10-50)	6.90%	8
Medium (51-250)	12.93%	15
Large (>250)	80.17%	93

Figure 1 - Answers to Question 1

According to the survey respondents, from the 116 professionals that answered, 80% are working in big companies while 20% correspond to companies with less than or equal to 250 employees.

- Question 2: In which sector is your company?



ANSWER CHOICES	RESPONSES	
Bank	18.10%	21
Health	4.31%	5
Insurance	5.17%	6
Transports	0.86%	1
Technology	36.21%	42
Other (which one?)	35.34%	41

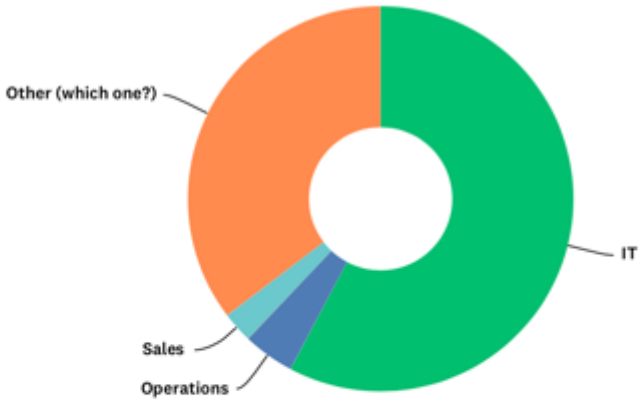
Figure 2 - Answers to Question 2

Since the survey respondents belong to different areas, and to have a set of specific clusters for each area, the researcher suggested a split as follows: Bank and Insurance,

Consumer Goods, Public Sector, Industry, Technology and Telecommunications, Health and Services.

Most of the respondents (39%) are from the Technology and Telecommunications sector; however, on the opposite side, we have the Health sector has proved to be one of the most vulnerable sectors and, simultaneously, one of the most targeted by hackers.

- Question 3: In which area of your company do you work?



ANSWER CHOICES	RESPONSES	
IT	57.76%	67
Operations	4.31%	5
Marketing	0.00%	0
Sales	2.59%	3
Other (which one?)	35.34%	41

Figure 3 - Answers to Question 3

The survey was conducted only to a specific audience: professionals that are responsible for handling their company's IT security. Within this cluster, most of the respondents (58,26%) were from the IT department and 22,4% of the remaining respondents that were professionals who worked directly in the information security/cybersecurity area.

- Question 4: Does your company have processes and policies relating cybersecurity?

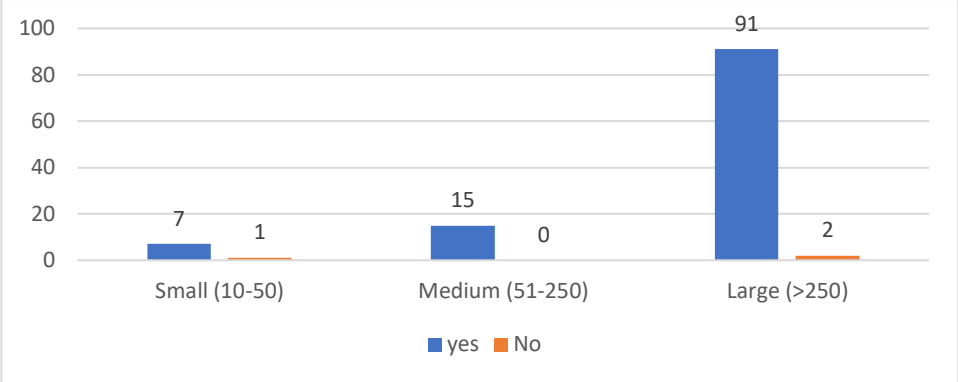


Figure 4 - Answers to Question 4

Out of 116 respondents, 98,25% of them had processes'. Only a small percentage of the total respondents, one small company and two large (1,75%) confirmed not to have any policies or processes to protect their business from possible threats.

- Question 5: Has your company ever been the victim of a cyber-attack?

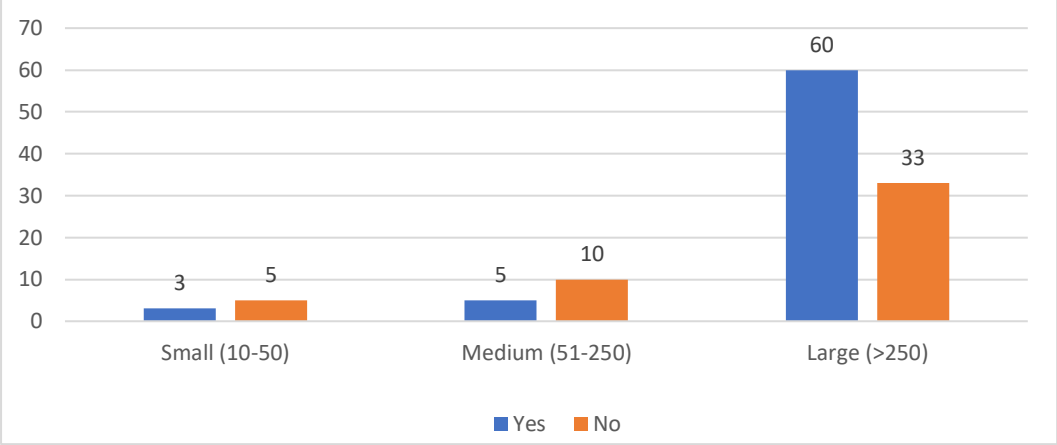


Figure 5 - Answers to Question 5

When the question was regarding companies being attacked, 57,14% of the respondents answered that they have, at some point, been attacked; however, some respondents refused to provide an answer – these will also be considered as being part of the respondents that answered yes. Since this question was somewhat controversial, the ones that did not respond will be regarded as individuals that belong to a company that has experienced some cybersecurity attack.

Additionally, when splitting the answer between the different size demographics, we can see that the larger companies are the ones being more victims of attacks with 52%.

- Question 6: Does your organization conduct system acquisition, development and maintenance?

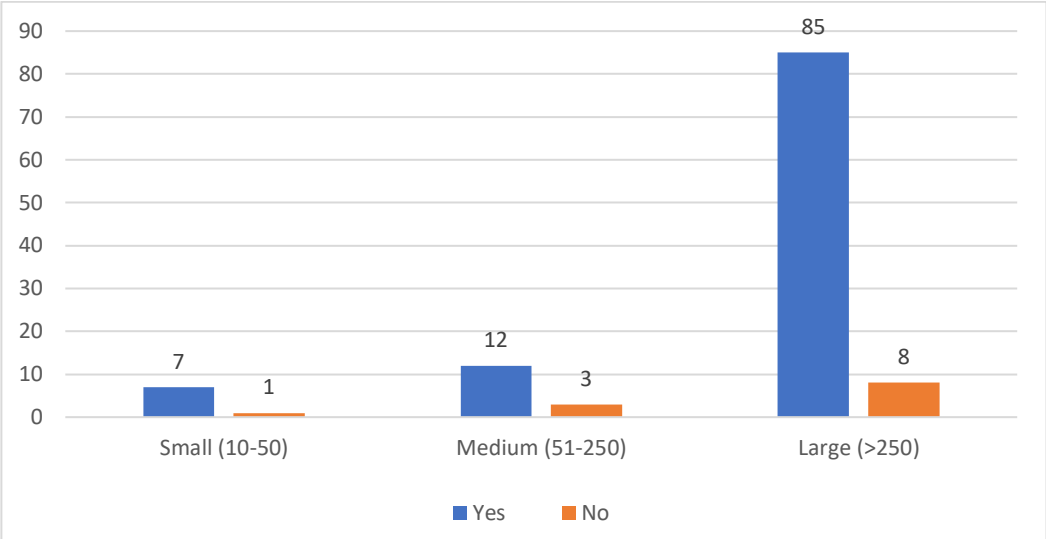


Figure 6 - Answers to Question 6

When asked if their organization buys, develops or maintains any systems, we can see that 90% of the organization's respondents have acquired these systems, as opposed to the remaining 9,7% that answered that their companies do not own any of these.

- Question 7: Does your organization have policies and processes in place to govern changes to all aspects of your IT infrastructure?

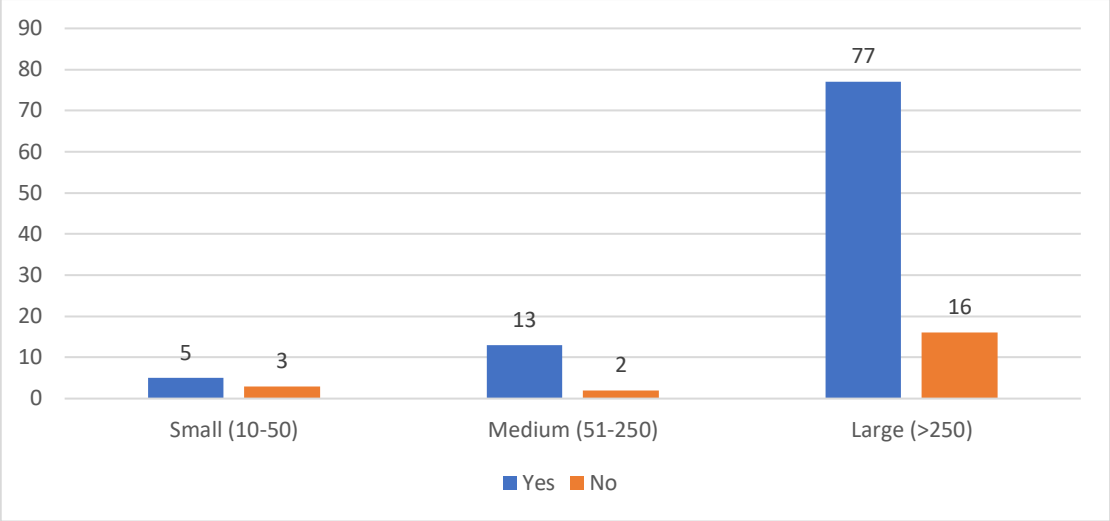
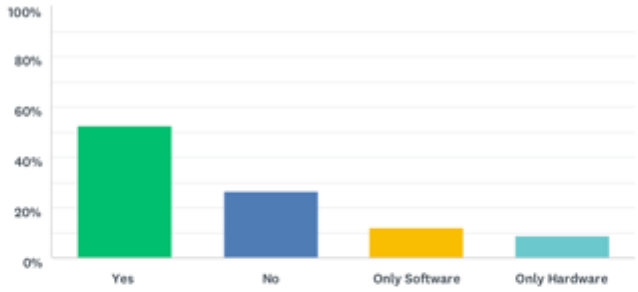


Figure 7 - Answers to Question 7

Through the respondents' feedback, we can see that most of the companies have in place security policies and processes to control any change on their IT infrastructure; however, 17,4% of the total respondents have confirmed not to have any to respond to these changes within their organization.

Further, we can see that the demographic size that has answered to not have in place these policies and processes are the Large companies.

- Question 8: Does your organization outsource software development and hardware acquisition?



ANSWER CHOICES	RESPONSES	
Yes	52.63%	60
No	26.32%	30
Only Software	12.28%	14
Only Hardware	8.77%	10

Figure 8 - Answers to Question 8

In terms of acquiring the software or hardware to a third party, most of the companies purchase both. However, a considerable percentage of the total respondents (26,32%) do not acquire any software or hardware. Additionally, we can verify that 12,28% buy only software from third party suppliers, while 8,77% purchase hardware only.

- Question 9: Does your organization require suppliers to adhere to an information security policy as part of supplier relationships?

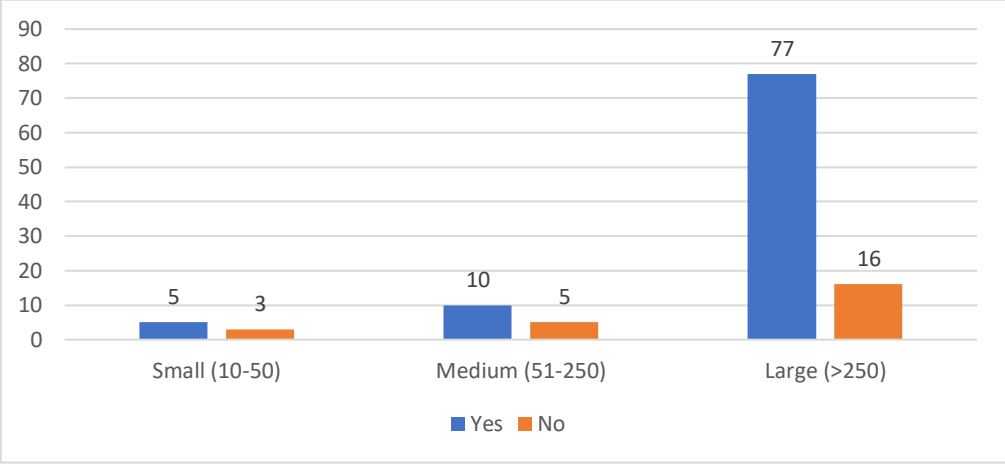
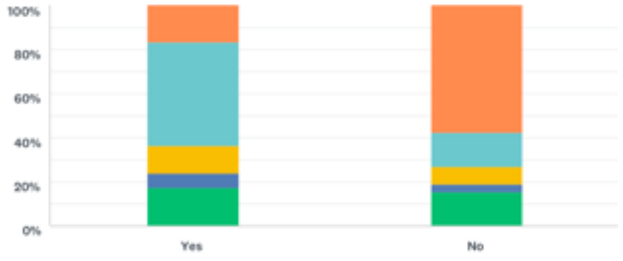


Figure 9 – Answers to Question 9

When confronted whether their companies require their third-party suppliers to adhere or follow any policies to protect their information, we can see that 80% of the respondents put this practice into place, as opposed to the remaining 20% who do not oblige their partners to have any rules or policies.

In this 20 %, although companies do not require when facing the number of affirmative answers with the negative ones we can see the is in the small and medium companies that these are the more sensitive.

- Question 10: Does your organization contract with third-party service providers and, if so, how regularly are contractor services monitored, reviewed, and audits carried out?



	MONTHLY	TRIMESTERLY	SEMESTERLY	YEARLY	N/A	TOTAL	WEIGHTED AVERAGE
Yes	17.58% 16	6.59% 6	12.09% 11	47.25% 43	16.48% 15	91	1.00
No	15.38% 4	3.85% 1	7.69% 2	15.38% 4	57.69% 15	26	1.00

Figure 10 – Answers to Question 10

To better understand the relationship between companies and their corresponding partners, the respondents answered whether they contract these third-party services and how often these are reviewed.

The results show that 78,4% (which is the equivalent to 91 respondents) do contract with third-party services. From these, 47,25% review the contract yearly and the ones that do not carry any reviewing were almost 16,5%.

However, the percentage of respondents that do not contract with third-party services was 24,1%, representing a total of 28 individuals. For the record, the ones that skipped this question were considered respondents that do not contract any third-party services at all.

- Question 11: Do information security considerations form part of your overall sourcing and supplier management activities?

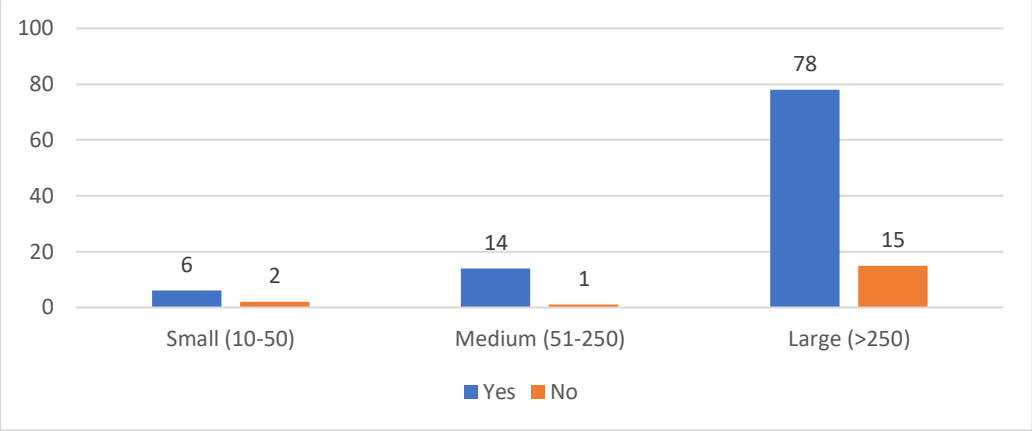


Figure 11 - Answers to Question 11

When inquired about whether information security is part of the respondents' company's process regarding their supplier management and sourcing, 86,73% of the respondents – which is the equivalent to 98 people – answered that information security is considered at their companies. However, 13,5% do not consider this as part of their companies' process; most of these were large companies. Furthermore, and for a more accurate analysis of this survey's data, those that skipped the question will be considered as individuals that belong to companies that do not take into consideration information security as part of their companies sourcing and supplier management activities.

- Question 12: Does your organization outsource to any third-party vendors who will have access to sensitive or critical assets or data (e.g. back up vendors, service providers, equipment support vendors, etc.)

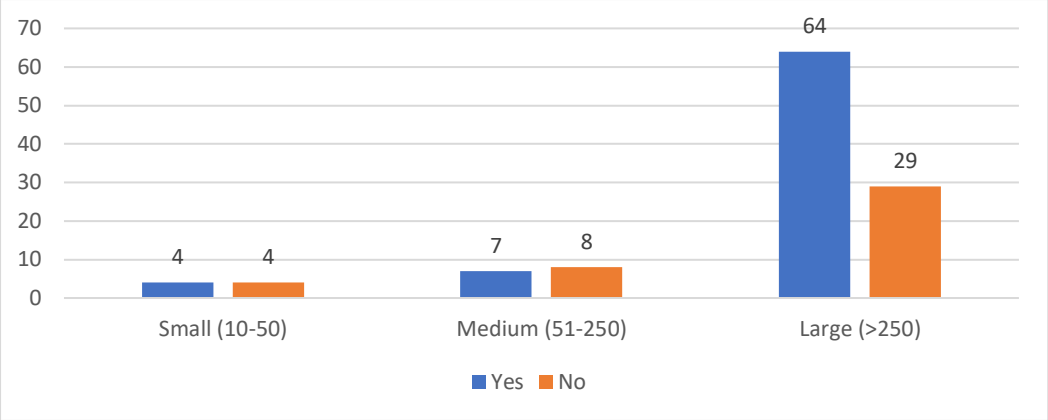


Figure 12 - Answers to Question 12

One of the things that information security focuses on is the sensitive data that might incur significant losses to a company. As a result, knowing if third-party vendors have access to this is of high importance. When questioned about this topic specifically, we can see that 67,57% of the total respondents answered that they do outsource with third-party vendors that will have access to sensitive or critical data. From the ones that answer, no 55% are from large companies.

- Question 13: Does your organization have policies and processes to identify and respond to changes to supplier services?

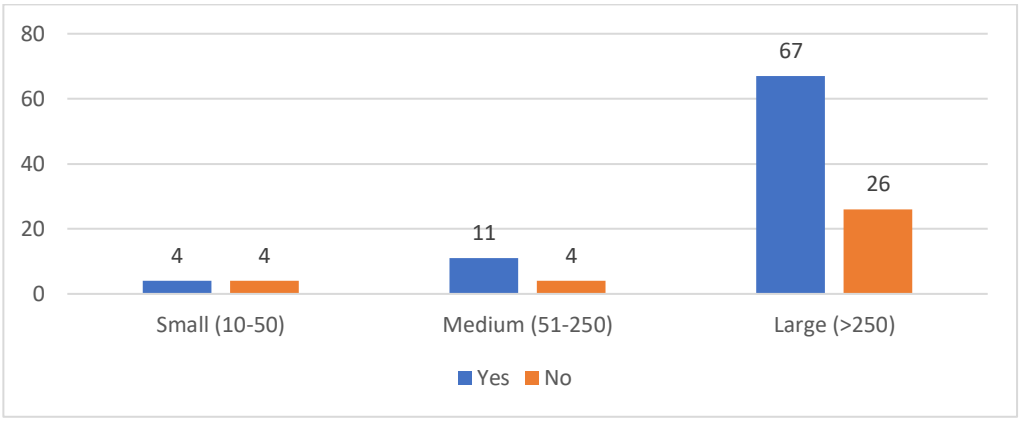


Figure 13 - Answers to Question 13

Information security is an area that is in constant shifting as a result of the rapid evolution of technology. For this reason, companies should establish internal processes and policies to follow the changes in their supplier services. When questioned whether the respondents' companies have any policies and processes to identify these changes, 29,3% of

the respondents (approximately 34 individuals) answered that they do not have any, where 26 are from large companies which represent the higher number.

- Question 14: Does your organization communicate Information Security policies and procedures to employees, contractors, customers and suppliers, and how is it communicated?

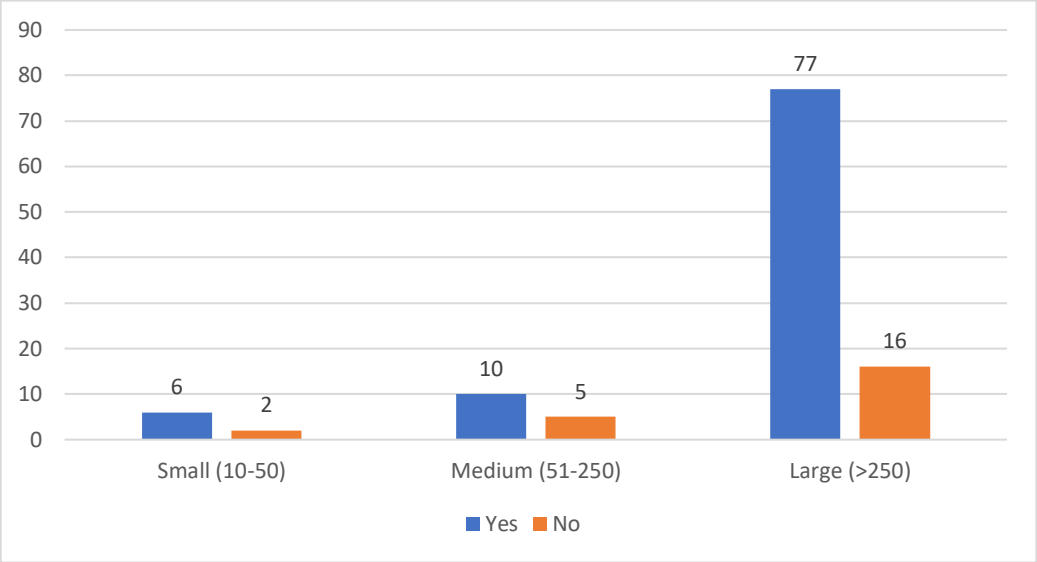


Figure 14 - Answers to Question 14

Information security policies & processes cannot be successfully implemented if companies do not communicate their policies and procedures to all the people that engage with the company.

When asking to the respondents what channels are used to communicate these policies and procedures, we find that the most common ways to communicate in small companies are: NDA (33%), Training and Emails each with 25%.

Regarding Medium companies, the ways to communicate are Email (46%), Training (16%), NDA (15%) and Intranet (11%).

Finally, when focusing on Large companies, the ways to communicate are Email (36%), Training (25,7%), NDA (19%) and Intranet (17%).

- Question 15: In your company is there a specific person with responsibility for ensuring that rules regarding third-party suppliers are adhered to and is it a requirement for that person to have any kind of training or certification (e.g. ISO)?

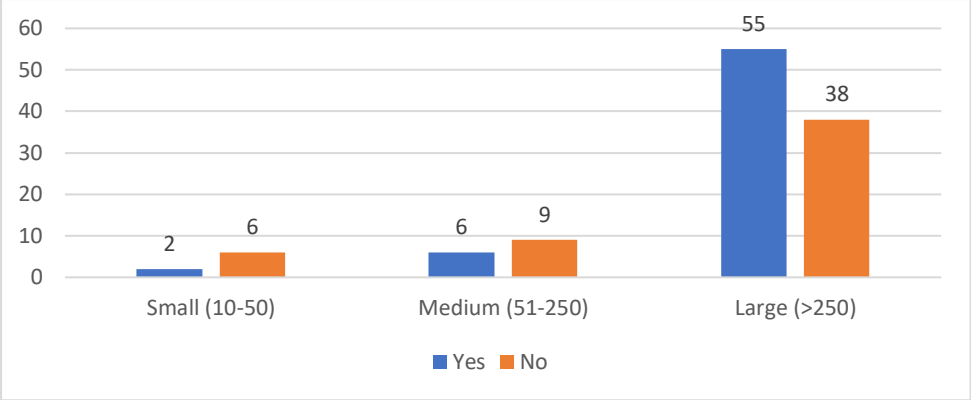


Figure 15 - Answers to Question 15

As previously discussed, – more specifically on the theoretical background section – not only is crucial that managers put into practice the policies and procedures regarding cybersecurity within the organization, but also their knowledge regarding the theme when it comes to frameworks and good practices. However, to understand who these managers were and what type of certifications or training they have acquired, this was questioned to the respondents. The results for this question show that in Small companies do not require any specific certification, and the person is not designated.

Regarding Medium companies, the person within the company that has the responsibility to ensure the established rules were adhered and put into practice is the CISO and CSM both with 16,7%. However, when referring to certifications required the ISO 27001 is the most required with 28%, then the ITIL framework with 8,3% and finally GDPR, CISM and CRISC - both with 3,33% each.

Finally, when focusing on Large companies the person with the responsibility to ensure that the established rules are adhered and put into practice is the CISO with 9,6%, the Information Security Officer and Compliance Specialist – both with 4,5% each, then the CSO with 4,2% and finally the Risk Management group and the Lawyer – both with 3,6% each.

Further, when understanding certifications, the ISO 27001 is the most implemented with 17,8%, the GDRP with 3,3% and finally ISC2 certifications like CISSP or SSCP with 2,9%. The higher percentage 29,1% - answered that there are no requirements for holding any certification.

- Question 16: If your organization has target systems that reside in a data centre, what kind of standards do you ask for? (somebody else's data centre)

Nowadays, one of the most used methods to both store and provide services is through the cloud; however, the security in the cloud is much often questioned regarding its actual security. When asked about this topic, 24% of the respondents confirmed not to have systems with their information on data centres, while 76% do have systems contracted with their own data centres. Regarding the standards that the companies ask for, the ISO 27000 is the most required one – representing 28% of the total answers. The other standards commonly asked for are the SOC/SSAE (13,8%) followed by the Tier classification of the data centres and a risk assessment (5%).

- Question 17: What evaluations do you do demand in case of trying to buy hardware/software from a third party?

When questioned about what kind of evaluations companies ask for in the process of buying hardware/software, we find that the most common answer is that corporate organizations do not have any evaluations – more precisely, this corresponds to a total of 42,2% of the respondents. However, the most common evaluations that companies ask for are Tender procedures (16,3%) – this includes license rights, warranty, product evaluation, SDLC and verified vendor distribution. The other evaluations that are typically asked are the ISO 27001 (13,7%), security policies (12%) and Risk Assessment (e.g., CAIQ) representing a total percentage of 8,6%.

5. Discussion

5.1. Discussion of Findings

Cybersecurity appears to be an area and a theme of great challenge and interest. As previously seen, although this area is associated with the IT area of the company, it should be treated as a whole separate area in a company. Though companies have policies and processes implemented, all of them are at risk, particularly the larger ones. Additionally, most of them have been, at some point in the time, attacked by threat actors, mainly the larger companies that medium or small ones. Although there are companies that have not been attacked sooner

or later, they will be. Still, it is the policies and processes implemented that will help the companies to respond and recover better from the attacks as also maintain the services resilient(Bank Of England, 2018; Financial Conduct Authority (FCA), 2019).

Nowadays, most companies have devices that run programs to perform their daily tasks which are going to be used by the employees. Before the usage of these devices, companies establish different policies and processes to perform their daily work in ways that would not cause harm to their organizational operations or at least that would not put them at risk.

To inform their employees regarding these policies and processes, each demographic size of the company applies different methods. The most used way to communicate in small companies is NDAs, on Medium size and Large size companies, communicate via Emails. Additionally, in Medium size and Large size training sessions are undertaken, which result in more direct contact with the company employees.

With all the changes that occur in the world of technology, these policies and procedures that are implemented protect not only the company but also prevent the changes in the IT infrastructure which is put in place by all the demographic size companies. There is a large number of large companies that do not have in place any policies or procedures to prevent changes.

This set of policies and procedures are also extended to third-party suppliers, in which these are mostly informed through non-disclosure agreements - these are mostly signed off on the act of doing the partnership between the companies that form the inter-organizational network.

As mentioned before, these policies and processes are applied usually by a specific manager and reviewed and audited yearly. Although this person gets in charge of implementing all of the necessary rules and strategies, they can only be successful if the ones that are being obliged to follow them understand the importance and need to comply with them.

As we could verify from the survey's responses, small size companies do not have any person responsible for the compliance of the cybersecurity processes. The non-existence of the manager has also led to the non-existence of requirements on specific training or certifications.

On medium size companies, we could verify that the managers within who are responsible for the compliance of the cybersecurity processes and policies are typically the CISO and the CSM. Regarding specific training or certifications, the ISO 27001 lead auditor

(which is the certification for auditors specialized in Information security management systems based on ISO 270001standard) as well ITIL framework is the most required.

Nevertheless, when focusing on the large size companies the manager responsible for the compliance of the policies and processes is the CISO, Compliance specialist or the Information Security Officer - these do not have mostly required specific training or certifications. However, the ones that require, ask for the ISO27001 lead auditor, as well as the ISC2 certifications like CISSP or SSCP and the GDPR, which is the regulation in EU regarding individual data protection.

When extending the interactions to the inter-organizational network, we found that companies oblige their partners – who act as a service supplier or hardware supplier – to adhere to information security. In other words, information security is a subject with high relevance to have efficient and successful inter-organizational network co-operations. There is still a large number of companies that do not oblige suppliers to adhere to information security.

These policies and procedures showed importance because suppliers will have access to sensitive data from the companies with whom they work; however, not only they have access to that data, but they will also have it stored in their Data Bases. Nevertheless, companies that have their IaaS/PaaS on third party providers are most attacked in spite of those that do not have it; this shows a new level of importance to the cooperation and security between companies. Regarding possible changes in the supplier services, there is a high number of companies that do not have any procedures to identify the changes put into place, most of these in the large size companies.

To work with these third-party suppliers, the companies' request for specific information security standards – that only apply to the security of the DB's – are usually the ISO 27000 compliance and SOC/SSAE compliance auditing.

Nevertheless, on the process of buying hardware or software from a third-party supplier, most the companies do not ask for any policies and procedures; however, there is still a small number of companies that usually ask for the tender processes.

5.2. Theoretical Implications

Although studied by researchers, there are no specific theories about cybersecurity when applied to the inter-organizational relationships between companies.

The most common approach is the deterrence theory; however, this approach is about human behaviour to deter certain practices and everyday routines. For this reason, it was not possible to get a wholly accurate understanding of feedback from the survey undertook from a user motivation point of view. Although we cannot address the motivation due to the nature of the enquiry, we found that certain good practices are not being applied.

Additionally, the survey conducted does not have a scientific base; hence, there are no scientific conclusions or implications to confront or associate as the analysis is only descriptive and based on standard procedures.

5.3. Organizational Design Implications

When trying to incorporate the inter-organizational relationships to the organizational design, we can say that managers should have more focus on their information security strategies. In other words, the Operational, Quality and Corporate governance should have implemented the information security effectiveness aligned with their business strategy. The inter-organizational relationships increase the attack vectors, which can reduce the business objectives (Gupta & Tarafdar, 2015; Srivastava & Kumar, 2015). Managers have one big task which is to protect their assets from any possible threat (internal or external), this should be made by understanding what the business processes are, assess them and reporting potential attack vectors to the Corporate Governance. It is in Corporate Governance that the company should rely on to be secure, this should gather the necessary resources whether is human resources or technological to deter or mitigate any situation that has been precepted by the Quality area. Corporate Governance area should actively participate in the assurance of control of the environment that protects their information assets

5.4. Managerial/Practical Implications

The present study might be one of the first to examine whether companies are concerned about their third-party suppliers having cybersecurity policies and procedures in place. The study has implications for research on managerial relevance and for search on how companies should address the cooperation between companies.

The results show that no matter what companies do at some point in time, all would be the target of an attack. Further, the results suggest that companies that cooperate with each other see that cybersecurity is a theme of great responsibility. However, when understanding more deeply the cooperation, that is being built between companies, these seem to be

requesting policies that are not aligned with the services provided by their third-parties. One of the very first things that companies should consider and implement within their businesses when it comes to cybersecurity and data protection the requirement of the minimum-security compliance standards. These should be both the ISO 27001 compliance for internal procedures and the SOC/SSAE for services, more specifically on the cloud. Also, not only the standards are necessary but also the internal processes are of high importance - e.g., monitoring employees when changing areas or leaving the company, controlling the software/hardware available and being used in the company to make sure that nothing is misplaced or that there is not an open door for attack vectors to access internal private data.

Secondly, the frequency of reviewing/auditing the policies and processes should be done on a more regular monthly basis – or, in worst-case scenarios, once every six months, – due to the fast pace of evolution of threats. Additionally, a verification of the software being used should be undertaken to verify if some available updates or patches need to be installed.

Finally, we found that most companies usually do not have an active member (manager-level individual) with any training or certification to be able to effectively take on the responsibility to implement the policies and procedures regarding cybersecurity on the interactions between companies. This aspect is one to change because companies cannot change the daily tasks (whether these are right or wrong) without one member to encourage and make everybody involved understand that these rules and strategies are seen as a benefit for the organization as a whole – after all, not only they save the companies from possible attacks but they also help the members of the organization to keep their jobs secure.

These should also focus their policies and processes in the recovery stage of an attack because companies will get hacked at some point of time and how well they are prepared to respond to it will be an advantage for them.

Managers should understand and keep in mind that for a company to be secure it is not only about securing their services but, most of the times, ensuring the business – which is done with the help of all of the involved members within the organization.

5.5. Limitations

The limitations of the present study are quite evident. Firstly, the paper focuses solely on studies regarding cybersecurity within the company context and not on the context of inter-organizational networks, precisely due to the lack of studies in the area. Secondly, the type of

questionnaire does not allow to undertake research based on scientific methods but only on procedures and the holistic understanding of the area through feedback provided by the survey's respondents. Thirdly, the survey included a few open-answer questions in which some respondents left the answers blank and, consequently, these could not have been taken into account – one of the reasons for skipping the questions might be because of the professional secrecy that the area obliges them to keep.

5.6. Future Research

The gathered data was used in clusters and was deliberately not focused on specific sectors to have a more focused set of responses. These sectors targeted seven main areas which resulted in a wide possibility for a more detailed analysis.

First, we are opening a new line of thinking for discussion and study of the reasons why the lack of abstraction for policies and processes implemented of third-party suppliers.

Second, on the basis of the results of this study, future research efforts could be devoted more profoundly to help the areas that are most targeted and most vulnerable to cyberattacks as also how companies should recover from a breach or an attack. Likewise, the understanding of profiling the risk/criticality of systems in an organization to allow these to protect themselves from significant business/reputational impact when hacked

6. Conclusion

The author of this research has sought to make a contribution to the cybersecurity literature in the broad domain of Cyber Governance and, more specifically, on the relationships between companies.

The study concluded that cybersecurity is a critical element in the daily life of companies; however, despite all the worries, companies are not being as cautious as they should with the security amongst the inter-organizational networks.

Hence, the companies that were enquired show preoccupation only regarding the provided services but not so much with the internal processes and procedures of their providers.

Although considered as a separate cluster in a company, Cyber Governance is not being applied as a whole. Furthermore, managers and qualified individuals are not being designated to face and overcome this challenge and, in most cases, they are not aware if their partners apply the same procedures and policies as them. Furthermore, they may even take for granted

that their partners have procedures and policies in practice without even enquiring them about those in the first place.

7. Appendix

7.1 Appendix A – Normalized Data

If your organisation contracts with third party service providers, how regularly are contractor services monitored, reviewed, and audits carried out?	Do information security considerations form part of your overall sourcing and supplier management activities?	Does your organization outsource to any third party vendors who will have access to sensitive or critical assets or data (e.g. back up vendors, service providers, equipment support vendors, etc.)	Does your organization have policies and processes to identify and respond to changes to supplier services?	Does your organization communicate Information Security policies and procedures to Employees, Contractors, Customers and Suppliers?	If your organization does communicate Information Security policies and procedures to Employees, Contractors, Customers and Suppliers how is it communicated?	In your company is there a specific person with responsibility for ensuring that rules regarding third-party suppliers are adhered to?
	Yes	Yes	Yes	Yes	We have our information portal for sharing this kinda things and awareness sessions quarterly,	No
	Yes	Yes	No	Yes	unregular study	No
Yearly	Yes	Yes	Yes	Yes	Web-based Trainings, mail, intranet, meetings	Yes
Monthly	Yes	No	Yes	Yes		Yes
Yearly	Yes	No	No	Yes	Information Security Awareness Trainings for employees. For others in contract(NDA or etc)	Yes
N/A	Yes	No	No	Yes	Through the scope of work stipulated in the agreement.	No
Monthly	No	No	No	Yes	Our outsourcing employees and contractors staff are signs formally NDA	Yes
Yearly	Yes	Yes	Yes	Yes	Online training, newsletters, security campaigns	Yes
	No	Yes	No	Yes	Company asks to sign printouts with policy requirements, without clarification	No
Monthly	Yes	Yes	Yes	Yes	Training sessions (Security Awareness)	Yes
Yearly	Yes	No	Yes	No		No
Yearly	Yes	No	Yes	Yes	They have to read them and sign the documents.	No
N/A	Yes	No	No	Yes	Intranet, emails	No
Yearly	Yes	Yes	Yes	Yes	kss, intranet portal, mail	Yes
	Yes	Yes	Yes	Yes	written	Yes
	Yes	Yes	Yes	Yes	agreement and awareness and review	Yes
Yearly	Yes	No	Yes	Yes	E-mails.	Yes
Yearly	Yes	Yes	Yes	Yes	IS Awareness activities (trainings, newsletters, direct email)	Yes
Yearly	Yes	No	No	Yes	Email and Intranet	No
Yearly	Yes	Yes	Yes	Yes	Private info	Yes
Yearly	Yes	Yes	Yes	Yes	Via e-mail	No
Semesterly	Yes	No	Yes	Yes	Web-form an application, RFI etc.	Yes
	Yes	Yes	No	Yes	To Employees by email with link directed to shared resource	No
Yearly	Yes	Yes	Yes	Yes	Courses, training and newsletters	No
	Yes	Yes	Yes	No		No
N/A	Yes	No	Yes	Yes	confidential	Yes
	Yes	No	Yes	No	-	Yes
Trimesterly	Yes	Yes	Yes	Yes	Cybergames, internal sessions and workplace training	Yes
Yearly	Yes	Yes	Yes	Yes	Contract	Yes
Semesterly	Yes	Yes	Yes	Yes	Intranet, email	Yes
Monthly	Yes	Yes	Yes	Yes	Regular communications and for each change, single source of policies.	No
Monthly	No	Yes	Yes	Yes	All our policies are available at our Intranet, and also through specific repositories to share with customers/providers	No
				Yes	NDA, Contratos, E-mail	Yes
	Yes	No	Yes	Yes	There is an awareness and training program, which use different communication ways, deppending on the objective to achieve, the context and the audience.	Yes
Yearly	Yes	Yes	Yes	Yes	documents and training	Yes
Monthly	Yes	Yes	Yes	Yes	As the relationship is initiated and annually or with any substantive change.	Yes
Yearly	Yes	No	No	Yes	Sing NDA	No
Yearly	Yes	Yes	Yes	No		No
Trimesterly	Yes	No	Yes	Yes	Through internal campaigns and disclosure with mandatory and digitally signed reading at the end of the training.	Yes
Yearly	Yes	Yes	No	No		No
Monthly	Yes	Yes	Yes	Yes	email, policy review, training	Yes
Semesterly	Yes	Yes	Yes	Yes	All third parties must sign NDAs (corporate and per user) and receive a copy of the relevant Policies and Procedures. On signitg the NDA their acknowledgement and knowledge of the contents of all documwnts are enforceable by law and in the court of law. They receive constant	Yes
Yearly	Yes	Yes	No	Yes	Documents have to be signed updates are circulated over email.	Yes
Yearly	Yes	Yes	Yes	No		No
Semesterly	Yes	Yes	Yes	No		No
	Yes	No	Yes	Yes	Conf	Yes
Yearly	Yes	Yes	Yes	No		No
Yearly	Yes	Yes	No	Yes	Security awareness campaign and a forma sign in Information security Policy.	Yes
	Yes	No	Yes	Yes	Staff meetings and e-mail broadcasts.	No
	No	Yes	No	No		No
	Yes	No	No	Yes	Any e-mail is being send to employee with written policies for all the employees to abide by it.	No
	Yes	No	Yes	Yes	Paper that must be acknowledged and signed	No
Semesterly	Yes	Yes	Yes	Yes	Email and intranet portal	Yes
	Yes	Yes	Yes	Yes	Emails and Intranet	Yes
Yearly	Yes	Yes	Yes	Yes	For internal employee by doing socialization meeting and discussion. For new employee by doing IT Security Awareness Socialization. For supplier by discussing or applying requirement that aligned with cyber security policy. For customer by adding some term	Yes
Trimesterly	Yes	Yes	Yes	Yes	NA	
Trimesterly	Yes	Yes	Yes	Yes	Via direct contract (paper)	Yes
Yearly	Yes	No	Yes	No		No
Semesterly	Yes	No	Yes	Yes	Many ways	Yes
	Yes	Yes	Yes	Yes	Contract clauses	No
	Yes	Yes	Yes	Yes	To employees is performed by training. Suppliers by email prior to any purchase or review.	No
	Yes	Yes	No	Yes	E-mail; Employee Portal;	Yes
Monthly	Yes	Yes	Yes	Yes	communications by mail, training, awareness sessions	Yes
	Yes	Yes	Yes	Yes	Training	Yes
	Yes	Yes	No	Yes	Portal.	No
Yearly	Yes	Yes	Yes	No		Yes
Yearly	Yes	Yes	No	Yes	E-mail	Yes
Yearly	Yes	Yes	No	Yes	Data Processing Agreemnets; Trainning	Yes
Yearly	Yes	Yes	No	Yes	Internal communication for the employees, web site to customers	Yes
Yearly	Yes	No	No	Yes	Everytime significant changes happen in this context, everyone that is impacted is briefed towards the new MO (e.g., GRPD).	No
Yearly	Yes	No	Yes	Yes	Intranet, emails, presential communication...	No
Yearly	No	Yes	Yes	No	e-mail and meeting	Yes
Monthly	Yes	Yes	Yes	No		No
Yearly	No	Yes	Yes	No		No
Semesterly	Yes	Yes	Yes	Yes	For our suppliers we include clauses on the contracts. For employees we have an awareness program and every year they have to accept the policies (internal WF)	Yes
Yearly						
Monthly	Yes	Yes	Yes	Yes	Shared documents, training, meetings	Yes
Monthly	Yes	Yes	Yes	Yes	Email and a notification letter at certain times. Also in contracts we provide.	Yes
	Yes	No	No	No		No
Yearly	Yes	Yes	Yes	Yes	We have several internal regulations and legal agreements with third parties.	Yes
Monthly	Yes	Yes	Yes	Yes	Onboarding read and sign, awareness actions, compliance reviews, regular training, available consulting on intranet.	Yes
	No	No	No	Yes	Awareness sessions	No
	No	Yes	No	No		No
Yearly	No	No	Yes	No		No
Semesterly	Yes	Yes	Yes	Yes	Onbording and periÃ³dica refresh courses	Yes
	No	Yes	Yes	No		Yes
	Yes	Yes	Yes	Yes	Email	No
	Yes	Yes	No	Yes	Email	Yes
Monthly	No	Yes	Yes	Yes	Training	Yes
Monthly	Yes	Yes	Yes	Yes	Email and internal communications.	No
Monthly	Yes	No	Yes	Yes	intranet and email	No
	Yes	Yes	Yes	Yes	Intranet, awareness sessions, ...	No
Monthly	Yes	No	Yes	Yes	By security awareness regular programs, before a celebration of a contract and when a new employee is admitted in the company.	Yes
Yearly	Yes	Yes	No	Yes	Mail, awareness sessions, contract clauses	Yes
Semesterly	Yes	Yes	Yes	Yes	Intranet	Yes
Semesterly	Yes		Yes	Yes	Mandatory Training, e-mails, Intranet	Yes
	Yes				.	
Yearly	Yes	No	Yes	No		No
			Yes	Yes	Welcome Pack + Compliance Training + Intranet	
Yearly	Yes	No	Yes	Yes	Training Acceptance of policies	Yes
Monthly	Yes	Yes	No	Yes	Intranet, Training	No
	Yes	Yes	Yes	Yes	Online training, Intranet, e-mails...	
Yearly	Yes	Yes	Yes	Yes	Yearly or after any change in policy. Changes are communicated by email to all employees.	Yes
Trimesterly	Yes	No	Yes	Yes	Online traiming	Yes
	Yes	No	Yes	Yes	email	Yes
Yearly	No	No	No	No		No
Trimesterly	Yes	No	Yes	Yes	Through email and pdf forms.	Yes
Semesterly	Yes	Yes	Yes	Yes	email, written contracts	No
Yearly	Yes	Yes	Yes	Yes	Memos, Intranet	Yes
Yearly	No	Yes	No	No		No
Yearly	Yes	No	No	Yes	Depends on the subject but mostly through a dedicated Cybersecurity section on our Intranet.	No
Yearly	Yes	Yes	No	Yes	Training - only to employees	No
	No	Yes	Yes	Yes	Contract agreement | training	No
	Yes	Yes	Yes	No	Tbd	No
	No	Yes	No	No		No
	Yes	No	Yes	No		No

If your company has a specific person with responsibility for ensuring that rules regarding third-party suppliers are adhered to is it a requirement for that person to have any kind of training or certification (e.g. ISO) ?	Does your organisation has target systems that reside in a data centre? (somebody else's data centre)	If your organisation has target systems that reside in a data centre, what kind of standards do you ask for? (somebody else's data centre)	Do you demand evaluations in case of trying to buy hardware/software from a third party?	What evaluations do you do demand in case of trying to buy hardware/software from a third party?
	Yes	ISO 27001	Yes	Brand reputation
	Yes	TIER	Yes	tender procedures
ISO27001	Yes	TIA, SOC	Yes	ISO27001, IEC 62443
yes	Yes	yes	yes	yes
Iso 27001 and etc	Yes	I can not answer it	Yes	Information Security standards
	Yes	Uptime / TIA	Yes	Meet the requirements such as security, functionality, and capability to be integrated with other solutions.
CISSP or CISA certifications are be preferred	Yes	verified certificate of "Tier III"	Yes	a trial period of using software from two months and a hardware warranty for a year, license rights and verified distribution by vendor
ISO, NIST, PCI	No		No	N/A
	Yes	ISO 9000	Yes	Price matching only
Certification not needed, but preferred.	Yes	ISO 27001 certification, TVRA reports	Yes	Supplier and product evaluation which includes usage within the financial industry
	No		Yes	Purchases and updates hardware/software performed regularly.
	Yes	Nobody can get in alone, they have to be escorted all the time.	No	
	Yes	ISO 27001	Yes	Not my area of responsibility
GDPR	Yes	ISO 27001, TIER (UpTime)	Yes	risk assessment
The company was not requiring any training. I was the one and took care of getting CISSP training and others When I was restructured, this was given to low cost person not having any IT experience (not able to recognize a network cable or USB key.) I wis	Yes	Same as in house	Yes	Long process with questionnaire
vendor risk management group	Yes	we have comprehensive questionaire to comply with various regulations	Yes	vendor risk management and procurement policy governs.
GDPR and ISO 27001	Yes	ISO 27001 and GDPR compliance.	Yes	Internal evaluation based on GDPR and security policy.
Information Security Officer is responsible for that and it is required to have ISO 27001 Lead Implementer certification.	Yes	TIA Tier I-IV	Yes	Checking the security certification of the hardware/software;
	Yes	Follow the NIST Framework.	Yes	* Search for faults. * Consult partner companies.
Private info	Yes	Usually SOC-2 audit reports or ISO 27k certification	Yes	Asked to complete security questionnaire or provide audit reports or certifications For some vendors executing a business associate agreement may be required if handling PHI Run POC
	Yes	SOC reports, ISO 27001	Yes	Level of SDLC and others software development maturity proofs.
ISO27001 Lead Auditor	Yes	ISO27001, SOC2, ISO27017 and 27018	Yes	RFI with security questionnaire and certificates
	Yes	N/A, we use AWS	No	No
	Yes	DR	Yes	vendor verification, test code quality
	Yes	Certifications	Yes	27001, ISO9001
confidential	No		Yes	none.....we prefer inbuilt
CISO	No		No	
DPO, CISO, CSO	Yes	GDPR, ISO 22K, ISO 27K	Yes	GDPR compliance and ISO 27K
Iso others	No		Yes	Sec
There is a person, but no specific training is required	Yes	ISO 27001 ISO 22301	Yes	Solutions certified by third parties
	Yes	ISO22301, Star (CSA)	Yes	Lots of them, but at the end we have an internal application certification which applies to both hw and sw.
	Yes	ISO Standards. (ISO27001 and others)	Yes	Right now, just a small test, but it's not enough ans we want to add additional evaluations.
Suprimentos	Yes	ISO 27001	Yes	Teste de invasÃ£o e anÃ¡lise de vulnerabilidades
local information security standards	Yes	ISO27000, local information security standards	Yes	we run a risk analisys to know that
CISSP, CTPRP, CISM	Yes	3rd party risk assessment process, plus SSAE docs, onsite review	Yes	static code analysis, dynamic test for SW onsite 3rd party review depending on criticality
We have a Compliance specialist and this person has ISC2 certs. (SSCP, CISSP)	Yes	Uptime guarantee - SLA, MSA, Privacy - NDA, MSA, Security SOC/ Our internal Assessment Questionnaire	Yes	We do our own due diligence, setup trial periods of testing, require our minimum security guidelines are met and adhered to as well as the items in #16.
	Yes	tier	Yes	Depends, we define the requisitions in the RFP
	No		No	
Professional information security	Yes	ISO 27000 Family and other market best practices	Yes	We do not purchase third-party hardware and software
	Yes	ISO 27001	No	
there is a person but not certification is required	Yes	conduct vendor risk assessment	No	
The SISO	Yes	We are flexible to the frameworks they use, but we demand to know all the controls and follow them closely.	Yes	Lots of testing on our part.
CISO	Yes	SOC 2 Type 2 compliant, ISO27001 minimum	No	Uncertain
	No		No	
	Yes	Border Security, Cybersecurity controls, Iso27001, Isae3402/sas70	Yes	lgpd (similar a European Gdpr)
Conf	Yes	Conf	No	
	No		No	
Its is asked and check in vendor assessment process.	Yes	It is made a vendor assessment and a security minimum requirements assessment based in ISO 27001.	Yes	Vendor assessment and a security minimum requirements assessment based in ISO 27001.
	No		No	
	No		No	
I am new in my company . I work as a consultant and this is a very small start up company	No		N/A	
	No		No	
Cism	Yes	Regional legislation compliance/legal iso	Yes	Before try anithing we see the capabilities and if not conflit with other software in house
ISO 27001	No		yes	Checklist about quality and security
IT Vendor & Asset Management, but our requirement for this function still not requiring any certification yet.	Yes	I do not understand the last senteces in the brackets. It might mean whether if we have any data center managed by third party right? We still have no policy that refer to any data center management standardization.	No	
.	No		No	
ISO, GDPR, SOX	Yes	Firewall, IAM, Strong Authentication, Audit	No	
	No		No	
Many	Yes	Many (security, continuity, risk, privacy, control, etc.)	Yes	Many (regulatory, standard, internal policies, control framwork, etc.)
	No		Yes	Only business related requirements until now
	Yes	ISAE3402, ISO	Yes	through security assessment and supplier assessment
Compliance Officer; DPO;	No		No	
CyberSecurity Manager	Yes	ISO27001; PCI	Yes	ISO27001; PCI
CISO	No		No	
	No		No	
DPO and INFOSEC Officer and COMSEC Officer	No		Yes	certification, compliance with best practices and ISO's
Infernal defined rules	Yes	SOC compliance	Yes	Depende on the project bought
ISO 27001 Lead Auditor; CISM; CISA; CRISC; CGEIT	No		No	
No specific training	Yes	No specific standard	Yes	Varies depending on the type of hw/sw to be bought from a third party
	No		Yes	Approval from IT/IS head and/or IT supplier.
	Yes	27001, 31000, 9001	Yes	It will depend on several (project) factors, context and goals
no certification	Yes	yes, nist.	Yes	we followed some recommendations of best market practices. certifications, security controls, infrastructure. we have a document that lists all the requirements.
	Yes	Soc rep	Yes	Caiq
	No		Yes	Security benchnark
The security team with procurement	Yes	Certifications, audit reports and others	Yes	Third party evaluation and financial stability and due diligence questionares
	No		No	
ANY	Yes	SSAE18, etc	No	
Legal department, Compliance team.	Yes	Unsure; I suppose systems that adhere and allow our systems to run?	Yes	That the product can be used by us; if hardware, that it is compatible with current systems, which we do an evaluation of before we even ask for the item.
	No		No	
Lawyers	Yes	ISO27Kseries, SOC, ISO9001, etc	Yes	ISO27001, 9001, ISO22301, etc
CISO	Yes	Tier IV Design & Facility certifications (delivered by Uptime Institute), ISO 27001/ISO 20000/ISO 14001/ISO 50001/ISO 9001	Yes	DÃ©pends of requirement's
	No		No	Na
	No		No	
	No		No	
Compliance	No		No	
CISO	Yes	Iso27799	Yes	CMMI
	No		No	
ISO, ITIL	Yes	ISO	Yes	price, technology
CSO	No		No	
	No		No	
	No		No	
	No		Yes	Our dept: security testing (pentesting)
Colleagues from Compliance and Cybersecurity departments	Yes	Don't understood what you mean by "standards". In banking area, there is a international standard called PCI-DSS every financial and banking company has to be compliant with.	Yes	The delivery has to be validated in its integrity. It can't be modified or opened until it arrives to the company, and the acceptance, storage and installation has to be validated by dual control (by two different persons)
There's no formal requirement on the training, but our Security staff has several certifications (CISSP, CCISO, ISO27001 Lead Auditor, etc.)	Yes	ISO2700x	Yes	Greatly depends on what we are buying. e.g.: software always hoes through Source Code review, Vulnerability assessment and Pentesting
Risk Management	No		No	
It depends of the scope. Data Centre? Risk Management? Others...	No		No	
.	No	.	No	.
	No		No	
	No		No	
27001	No		No	
	No		Yes	CIS Hardening
.	No		No	
ISO 27001 Lead Auditor.	Yes	PCI DSS, SOC 2, ISO 27001 at least.	Yes	Review their policies and procedures annually. Request the latest penetration tests results.
ISO, CISSP, NIST	No		No	
ISO	Yes	ISO	Yes	ISO
		SOC1 type II	No	
ISO 9k, 10k, 14k, 27k1, CRISC, CISM, CISA, GDPR	Yes	At least 27k1 but not limited only with that	Yes	Standards & complements
	No		No	
ISO, DPO	Yes	There is process for risk evaluation, mitigation and acceptance.	Yes	Depends on the purpose, criticality..
	Yes	ISO 27001	Yes	Policies and Security Guidelines
	No		Yes	We've begun to ask for internal audit reports and internal cybersecurity policies.
	No	NA	Yes	It depends: A+, CCT..
	No		No	
	No	N/a	No	
	No		No	
	No		No	

7.2. Appendix B – Survey

Cybersecurity Questionnaire - Supplier Relationships

Este questionário enquadra-se num estudo desenvolvido no âmbito de uma tese de mestrado da Nova IMS - Nova Information Management School e tem como foco perceber a relação entre empresas relativamente a cybersegurança.

Para quaisquer dúvidas e/ou questões, não hesite contactar m20170416@novaims.unl.pt.
Obrigada pela colaboração

This questionnaire is part of a study developed within the framework of a master's thesis of Nova IMS - Nova Information Management School and aims to understand the relationship between companies in cybersecurity.

For any questions and/or questions, do not hesitate to contact m20170416@novaims.unl.pt.
Thank you for your cooperation.

1. What is your company size?

- [ ] Small (10-50)
- [ ] Medium (51-250)
- [ ] Large (>250)

2. In which sector is your company?

- ◯ Bank
- ◯ Transports
- ◯ Health
- ◯ Technology
- ◯ Insurance
- ◯ Other (which one?)

3. In which area of your company do you Work?

- ◯ IT
- ◯ Marketing
- ◯ Operations
- ◯ Sales
- ◯ Other (which one?)

4. Does your company have Processes and Policies relating cybersecurity?

- ◯ Yes
- ◯ No

5. Has your company ever been the victim of a cyber attack?

- ◯ Yes
- ◯ No

6. Does your organisation conduct System Acquisition, Development and Maintenance?

- ◯ Yes
- ◯ No

7. Does your organization have Policies and Processes in place to control government changes to all aspects of your IT infrastructure?

- ◯ Yes
- ◯ No

8. Does your organization outsource software development and Hardware acquisition?

- ◯ Yes
- ◯ No
- ◯ Only Software
- ◯ Only Hardware

9. Does Your organization require suppliers to adhere to an Information Security policy as part of supplier relationships?

- ◯ Yes
- ◯ No

10. Does your organisation contract with third party service providers and if so, how regularly are contractor services monitored, reviewed, and audits are carried out?

	Monthly	Trimesterly	Semesterly	Yearly	N/A
Yes	◯	◯	◯	◯	◯
No	◯	◯	◯	◯	◯

11. Do information security considerations form part of your overall sourcing and supplier management activities?

- ◯ Yes
- ◯ No

12. Does your organization outsource to any third party vendors who will have access to sensitive or critical assets or data (e.g. back up vendors, service providers, equipment support vendors, etc.)

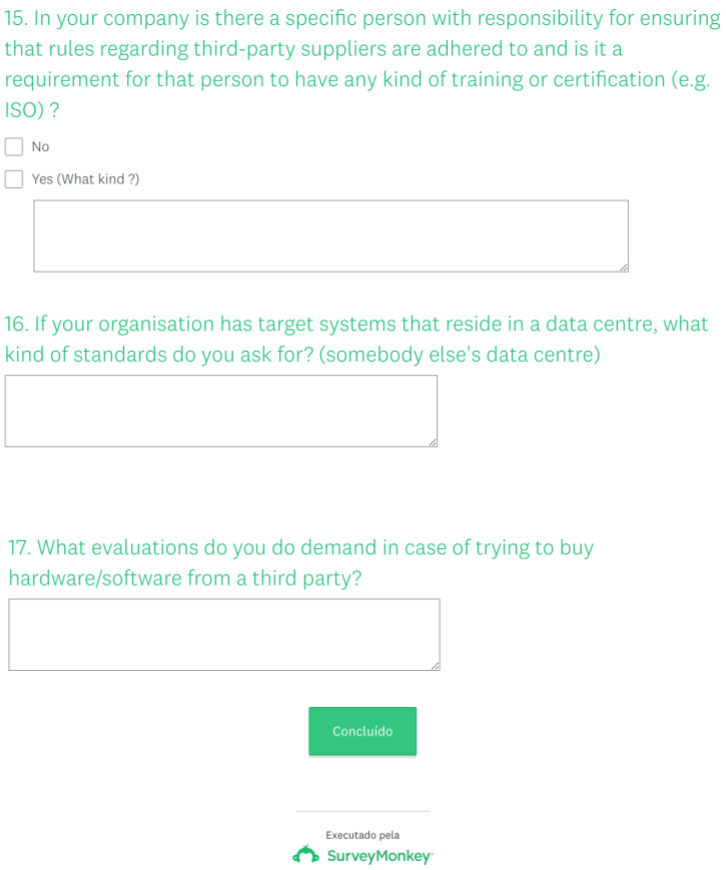
- ◯ Yes
- ◯ No

13. Does your organization have policies and processes to identify and respond to changes to supplier services?

- ◯ Yes
- ◯ No

14. Does your organization communicate Information Security policies and procedures to Employees, Contractors, Customers and Suppliers and how is it communicated?

- ☐ No
- ☐ Yes (How?)



8. References

Afuah, A. (2003). Redefining Firm Boundaries in the Face of the Internet: Are Firms Really Shrinking? *Academy of Management Review*, *28*(1), 34–53. https://doi.org/10.5465/AMR.2003.8925207

Anderson, C., Baskerville, R. L., & Kaul, M. (2017). Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. *Journal of Management Information Systems*, *34*(4), 1082–1112. https://doi.org/10.1080/07421222.2017.1394063

Bagchi, K., & Udo, G. (2003). An Analysis of the Growth of Computer and Internet Security Breaches. *Communications of the Association for Information Systems*, *12*, 19.

Baker, W. E., & Faulkner, R. R. (2017). Interorganizational Networks. In *The Blackwell Companion to Organizations* (pp. 520–540). https://doi.org/10.1002/9781405164061.ch22

Bank Of England. (2018). *PRA Business Plan 2018/19*. 24.

Benaroch, M., & Chernobai, A. (2017). Operational It Failures, It Value Destruction, and Board-Level It Governance Changes. *MIS Quarterly*, *41*(3), 729.

Boockholdt, J. L. (1989). Implementing Security and Integrity in Micro-Mainframe Networks. *MIS Quarterly*, *13*(2), 135–144.

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011). Human Performance in Cybersecurity: A Research Agenda. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *55*(1), 1115–1119. https://doi.org/10.1177/1071181311551233

Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT. (2018, July 11). Retrieved November 25, 2018, from Security Intelligence website: https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use. *Journal of Management Information Systems*, *31*(4), 49–87. https://doi.org/10.1080/07421222.2014.1001257

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, *29*(3), 157–188.

Dey, D., Lahiri, A., & Zhang, G. (2012). Hacker Behavior, Network Effects, and the Security Software Market. *Journal of Management Information Systems*, *29*(2), 77–108.

Equifax breach could be most costly in corporate history. (2018, March 2). *Reuters*. Retrieved from https://www.reuters.com/article/us-equifax-cyber-idUSKCN1GE257

Equifax owes you a lot more, but here's how to get $125 from this week's settlement—The Verge. (n.d.). Retrieved July 25, 2019, from https://www.theverge.com/2019/7/25/8930233/equifax-data-breach-ftc-settlement-claim-sign-up-how-to

European Commission—PRESS RELEASES - Press release—General Data Protection Regulation shows results, but work needs to continue. (n.d.). Retrieved July 25, 2019, from http://europa.eu/rapid/press-release_IP-19-4449_en.htm

Financial Conduct Authority (FCA). (2019, June 20). Service standards 2018/19. Retrieved September 2, 2019, from FCA website: https://www.fca.org.uk/data/service-standards-2018-19

Galbreth, M. R., & Shor, M. (2010). The Impact of Malicious Agents on the Enterprise Software Industry. *MIS Quarterly*, *34*(3), 595-A10.

Gnyawali, D. R., & Madhavan, R. (2001). Cooperative Networks and Competitive Dynamics: A Structural Embeddedness Perspective. *Academy of Management Review*, *26*(3), 431–445. https://doi.org/10.5465/AMR.2001.4845820

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, *34*(3), 567-A2.

Gupta, J. D., Ofir Turel, and Ashish, & Tarafdar, M. (2015). The Dark Side of Information Technology. Retrieved July 25, 2019, from MIT Sloan Management Review website: https://sloanreview.mit.edu/article/the-dark-side-of-information-technology/

Håkansson, H., & Ford, D. (2002). How should companies interact in business networks? *Journal of Business Research*, *55*(2), 133–139. https://doi.org/10.1016/S0148-2963(00)00148-X

Harcourt, A. (2018). *SAMGarde-Cyber_Short_Course-Week1*.

Hui, K.-L., Kim, S. H., & Wang, Q.-H. (2017). Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. *MIS Quarterly*, *41*(2), 497-A11.

Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the Value of Countermeasure Portfolios in Information Systems Security. *Journal of Management Information Systems*, *25*(2), 241–279.

Lee, D.-J., Ahn, J.-H., & Bang, Y. (2011). Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection. *MIS Quarterly*, *35*(2), 423-A8.

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, *33*(1), 71–90.

Liang, N. (Peter), Biros, D. P., & Luse, A. (2016). An Empirical Validation of Malicious Insider Characteristics. *Journal of Management Information Systems*, *33*(2), 361.

Lucas Jr., H. C., Agarwal, R., Clemons, E. K., El Sawy, O. A., & Weber, B. (2013). Impactful Research on Transformational Information Technology: An Opportunity to Inform New Audiences. *MIS Quarterly*, *37*(2), 371–382.

Majchrzak, A., & Jarvenpaa, S. L. (2010). Safe Contexts for Interorganizational Collaborations Among Homeland Security Professionals. *Journal of Management Information Systems*, *27*(2), 55.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems*, *34*(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Poppensieker, T., & Riemenschnitter, R. (2018, March). A new posture for cybersecurity in a networked world | McKinsey. Retrieved October 6, 2018, from https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems*, *32*(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Shipilov, A., Gulati, R., Kilduff, M., Stan Li, & Wenpin Tsai. (2015). Relational Pluralism Within and Between Organizations. *Academy of Management Journal*, *1015*(1), 90–100. https://doi.org/10.5465/amj.2013.1145

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/10.2307/25750688

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, *20*(2), 167–196.

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly*, *34*(3), 503-A5.

Srivastava, H., & Kumar, S. A. (2015). Control Framework for Secure Cloud Computing. *Journal of Information Security*, *06*(01), 12–23. https://doi.org/10.4236/jis.2015.61002

Stafford, T. F., & Urbaczewski, A. (2004). Spyware: The Ghost in the Machine. *Communications of the Association for Information Systems*, *14*, 291–306. https://doi.org/10.17705/1CAIS.01415

Straub, D. W., & Welke, R. J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, *22*(4), 441–469.

Straub Jr., D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, *1*(3), 255–276. https://doi.org/10.1287/isre.1.3.255

Straub, Jr., Detmar W., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly*, *14*(1), 45–60.

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly*, *37*(1), 1–20.

Wolff, J. (2016). Perverse Effects in Defense of Computer Systems: When More Is Less. *Journal of Management Information Systems*, *33*(2), 597–620. https://doi.org/10.1080/07421222.2016.1205934

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements. *Journal of Management Information Systems*, *30*(1), 123–152. https://doi.org/10.2753/MIS0742-1222300104

Zviran, M., & Haga, W. J. (1999). Password Security: An Empirical Study. *Journal of Management Information Systems*, *15*(4), 161–185.

Hoffer. Jeffrey A. and Detmar W. Straub. "The 9 to 5 Underground: Are You Policing Computer Crimes?" Sloan Management Rev . 30 (1989). 35-44.