NOVA IMS Information Management School

MEGI

Mestrado em Estatística e Gestão de Informação

Master Program in Statistics and Information Management

Supply of cyber insurance in banking sector operating in Portugal

Ana Rita Batista Martins

Dissertation presented as the partial requirement for obtaining a Master's degree in Statistics and 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

SUPPLY OF CYBER INSURANCE IN BANKING SECTOR OPERATING IN PORTUGAL

Ana Rita Batista Martins

Dissertation presented as the partial requirement for obtaining a Master's degree in Statistics and Information Management, Specialization in Risk Analysis and Management

Advisor / Co-supervisor: Rui Alexandre Henriques Gonçalves

February 2020

ACKNOWLEDGEMENTS

I would like to thank and dedicate this master's thesis to the following people:

To my parents, Teresa and José, my sister, Cristina, my boyfriend, Henrique, for supporting me constantly and unconditionally in this stage. They are, without any doubt, the main pillars of fundamental strength and motivation for this work to end. All the hours dedicated to the thesis and abdicated in family time are reflected in this work and that is why I consider it a bit of all of us.

To my friends and colleagues who helped me contributing with ideas and solutions in times of doubts and uncertainties. In particular, to those who helped me promptly in the dissemination of my questionnaires.

To all participating insurance companies and, in particular, to their employees who were available to answer the questionnaire. To Dr. Luís Malcato and Dr. Miguel Guimarães, from APS, who helped me in spreading the questionnaire across the sector, thus giving a vote of confidence and recognition in my work.

To Dr. Hugo Borginho, from ASF, who made himself available, together with the collaborators most connected to the topic, to answer the questionnaire.

Finally, to my advisor, Professor Rui Gonçalves, for having accepted to guide my thesis, for given me the opportunity to participate in the 19th Portuguese Association of Information Systems Conference at Nova IMS and for having followed my work.

ABSTRACT

The development of technology and the way of doing business exchange sensitive information all over the world through IT resources. In consequence of such reality, cyber events are more likely to occur, being the banking sector one of the major targets. However, in parallel with these new perils from technological growth, awareness of cyber risk is also increasing among institutions, as well as the search for protection and measures to fight them. Cyber insurance is one of the possible protection options.

The main goal of this work is to assess the supply of cyber insurance among the banking sector operating in Portugal. As empirical investigations of cyber insurance applied in the country are rarely reported in the literature, the results are novel.

In order to get the main goal, the research is based on a literature review where will be presented the "state of the art" of cyber insurance market in the world and in the country. In addition, an empirical study will be made through the application of questionnaires to ascertain the specificities of cyber insurance suppliers or potential suppliers in the Portuguese market, their perception of market evolution and knowledge about cyber risk. There is also a specific questionnaire for the supervisor entity in order to know its point of view about the topic in discussion.

The main conclusions of this study relate to the fact that there is still a long way to go in the Portuguese insurance sector for cyber risk. The sector in the country started to be developed by international companies and only after that the national ones started to have more awareness on the subject, as mentioned by the Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF).

However, awareness of the issue is not the only point that leads to the underdevelopment of this specific insurance. The difficulties in the product underwriting process, which on the part of those who sell as well as those who buy, the high and variable prices, the lack of historical data and the information asymmetries are examples of obstacles that still have to be overcome.

Although the cyber risk insurance sector is taking its first steps, it is believed to have a large margin of expansion, as has already been the case in several other countries. The creation of information sharing platforms on cyber incidents and the design of insurance and reinsurance products for cyber incidents are considered by the participant insurers as the main measures to be taken to assist this market development. It therefore becomes an inevitable topic to be addressed by the insurance sector in Portugal.

KEYWORDS

Cyber Risk; Cyber Insurance; Operational Risk; Banking sector; Insurance sector

INDEX

LIST OF FIGURES

LIST OF TABLES

LIST OF ANNEXES

LIST OF ABBREVIATIONS AND ACRONYMS

ASF Autoridade de Supervisão de Seguros e Fundos de Pensões

ATM Automated Teller Machines

CBI Contingent Business Interruption

CEO Chief Executive Officer

CEPS Centre for European Policy Studies

CFO Chief Financial Officer

CIO Chief Information Officer

CISO Chief Information Security Officer

CISP Cyber security Information-Sharing Partnership

DDoS Distributed denial-of-service Attack

D&O Directors and Officer

DNS Domain Name System

DoS Denial-of-Service Attack

EBA European Banking Authority

ECRI European Credit Research Institute Brussels

EIOPA European Insurance and Occupational Pensions Authority

ENISA European Network and Information Security Agency

ERH Electronic Health Records

ESA European Supervisory Authorities

EU European Union

GDP Gross Domestic Product

GDPR General Data Protection Regulation

GLBA Gramm-Leach–Bliley Act

HIPAA Health Insurance Portability and Accountability Act

HITECH Health Information Technology for Economic and Clinical Health Act

IAIS International Association of Insurance Supervisors

ICT Information and communications technology

IoT Internet of Things

IP Internet Protocol

ISO International Organization for Standardization

IT Information Technology

ITU International Telecommunication Union

OECD Organization for Economic Co-operation and Development

OSP Outside Security Provider

OTP One Time Password

PCI-DSS Payment Card Industry Data Security Standard

PHI Personal Health Information

PII Personally Identifiable Information

POS Point-of-sale

SOX Sarbanes Oxley Act

SWIFT Society for Worldwide Interbank Financial Telecommunications

1. INTRODUCTION

Cyberspace and the internet have revolutionized the way of communication and do business. They enabled to expand interconnectivity as well provided several benefits for knowledge-based economies, allowing businesses to operate globally with greater speed and efficiency. But where there is a great opportunity, there are also risks associated with it (IRM, 2014). The rapid pace of technological change, increasing connectivity through the Internet of Things[1] (IoT) and the growing sophistication of cyber-attackers introduce new vulnerabilities and increase the potential for systemic and risk aggregation complexities (Camillo, 2017).

Approaches to cyber risk are maturing as organizations recognize it as an enterprise business risk and not just an information technology (IT) problem (Marsh & McLENNAN, 2018). There is also the acknowledgment that cyber risk cannot be completely eradicated from business because of its many correlations and specificities. The best that can be done is to be managed to facilitate the success of a company's drive forward (RSA, 2016).

Several possibilities to manage this risk have emerged along with the decision-maker awareness and understanding to it. Cyber insurance is one of the possibilities that was created to address risk that cannot be reasonably mitigated by IT security measures and because of the realization that current insurance policies may not adequately cover cyber risks (Biener, Eling, & Wirfs, 2014).

Also, in the area of supervision and regulation cyber risk is a growing concern. The European Union (EU) has made several efforts to harmonize rules and procedures through legislation and recommendations that aim to help organizations to protect themselves and be more aware of this new kind of threat.

Faced with the new perils, financial institutions like banks and insurers see in the need to rethink strategies in order to adapt to the new challenges imposed by technological innovation. Banking institutions (representing the demand side for the purpose of this work) need to find out how to manage these new risks and find the most efficient way to invest in security without losing profitability. This raises questions inside those institutions like are they sufficiently aware for cyber-attacks? Should the organization self-insure their exposure to cyber risk or should they buy insurance? How much they are willing to invest to transfer their exposure? What are the risks they expect to cover with insurance? On the other hand, insurance companies (representing the supply side) need to adjust to the new reality of threats and offer insurance that delivers what their customers need in terms of cyber perils but at the same time not jeopardizing their ability to accept risk. This arises questions like how much the company are willing to accept to take costumer's risk? What covers they are expecting that costumers will seek for? What cover limits the company impose? What requisites the company demand costumers to have in order to offer a cyber insurance product?

[1] There is no common definition for IoT. A definition proposed by The International Telecommunication Union (ITU) for instance defines it as ''a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies'' (Fluchter & Wortmann, 2015).

The main goal of this work is to assess the supply of cyber insurance among the banking sector operating in Portugal. As empirical investigations of cyber insurance applied in the country are rarely reported in the literature, the results are new.

The research is based on a literature review where will be presented the “state of the art” of cyber insurance market in the world. In addition, an empirical study will be made through the application of online questionnaires to ascertain the specificities of the market’s supply side players constituted by insurance companies working in Portugal. In addition, it will also be explored the Portuguese insurer's supervisor, Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF), view about the offer of an insurance against cyber risk for banking sector in the country.

In order to do that this work is be divided in six main chapters. Chapter 2 presents the study relevance where it is characterized the cyber risk around the world and in Portugal, explained the reason why it is a great concern and the main consequences of a cyber-attack. Chapter 3 describes the main goal of this work and the specific objectives to reach the key objective. The most extensive part of this work is disclosed in chapter 4. It is a literature review talking about cyber risk, cyber insurance, cybersecurity in banking sector and a quick overview about legislation. Chapters 5, 6 and 7 are the most practical ones. They describe the methodology applied, the results, discussion and main conclusions that resulted from the empirical investigation.

2. STUDY RELEVANCE

2.1. BACKGROUND

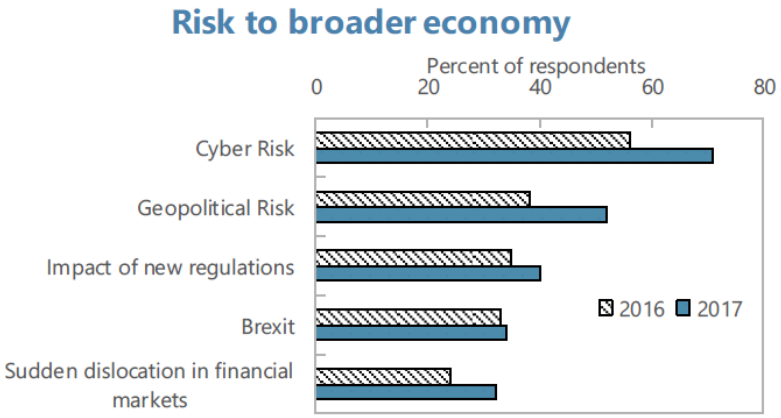
Electronic media is replacing the traditional approach of file and paper systems, so having information online for almost all the activities is the new trend emerging in world, which require high level of network availability and consequently high-level of system security (Saini, Azad, Raut, & Hadimani, 2011). Emerging technology such as Fintech[2] is an example of that. It is a new way of doing business that replaces bureaucracy and time-consuming processes by online procedures much faster and easier to get. Although technology innovations allow a wide range of possibilities for human progress, it also increases the vulnerability to cyber incidents once it expands the number of entry points into institutions, which hackers could target (IMF & Bouveret, 2018).

In short, as stated by Deloitte Advisory Cyber Risk Services in the RSA paper ("Cyber Risk Appetite: Defining and Understanding Risk in the Modern Enterprise."), "the fundamental things that organizations undertake in order to drive performance and execute on their business strategies happen to also be the things that actually create cyber risk. This includes globalization, mergers and acquisitions, extension of third-party networks and relationships, outsourcing, adoption of new technologies, movement to the cloud, or mobility" (RSA, 2016).

According several sources, through their researches and forums, the cyber risk is increasingly considered relevant and a concern. Technological risks, in the form of data fraud, cybersecurity incidents or infrastructure breakdown, were identified as among the top ten risks facing the global economy and the fourth largest risk among surveyed insurers by the International Association of Insurance Supervisors (IAIS, 2016). A year later, in the eighth Emerging Risks Survey by the Society of Actuaries, cyber risk was considered the greatest emerging risk (Xu, Hua, & ASA, 2017). Reaching the same conclusion, in the World Economic Forums[3] of 2012, 2014, 2017, 2018 and 2019, cyber-attacks were considered in the top 5 global risks in terms of likelihood. Additionally, a survey of the major risks to financial stability done by IMF verified that cyber risk was considered, in the past years of 2016 and 201, the greatest peril to stability among other risks like geopolitical, impact of new regulation or Brexit (IMF & Bouveret, 2018), as represented in figure 2.1 of risks to broader economy.

[2] FinTech Action plan: For a more competitive and innovative European financial sector. https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf

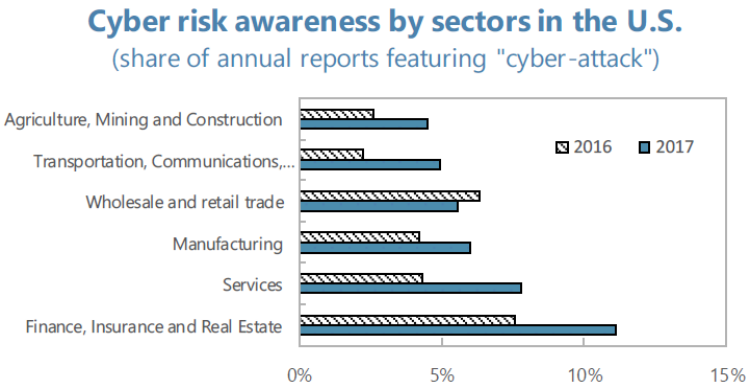
[3] World Economic Forum reports can be read at https://www.weforum.org/reports



Source: IMF, & Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. DTCC Systemic Risk barometer 2017Q1

Figure 2.1 Risk to broader economy

Cyber risk is transversal to all sectors of activity once all of them depend on IT resources and rely on customer's data to conduct business. Figure 2.2 shows an example of the awareness of cyber risk across several business sectors in the U.S. being the financial, insurance and real state sectors the most conscious (IMF & Bouveret, 2018).



Source: IMF, & Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.. SEC form 10-K; and staff calculations

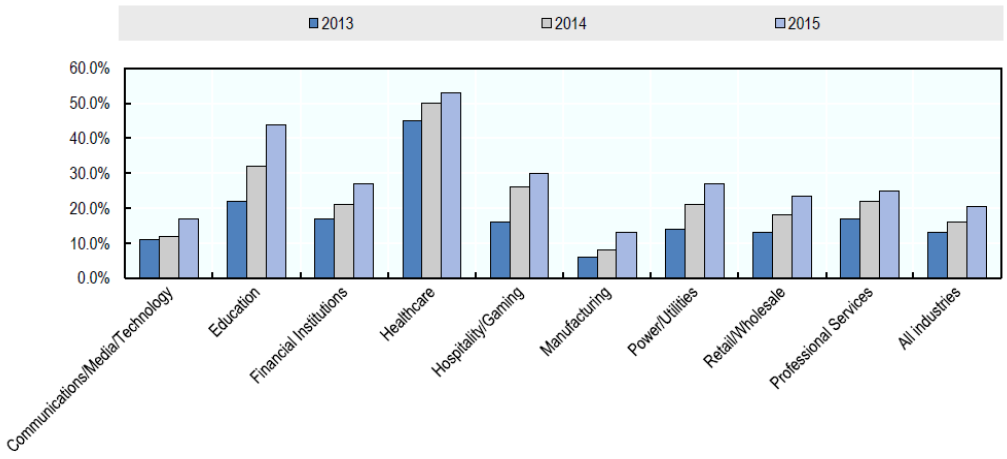
Figure 2.2 Cyber risk awareness by sector in the U.S.

In parallel to the rising awareness of cyber events, the penetration of cyber insurance is also increasing, representing one of the fastest growing sectors of the insurance industry, according to AIR 2017 estimates (AIR, 2017).

More specifically, following the beginning of year 2000, the dotcom crash and the September 11 attacks, interest in cyber insurance grew as there was a growing realization that the virtual world did not necessarily fit within the scope of many traditional covers/classes of insurance (Camillo, 2017).

According to European Network and Information Security Agency (ENISA), sectors typically buying cyber insurance include retailers, healthcare providers, hotels and financial services (ENISA, 2012). Noting the same, Organization for Economic Co-operation and Development (OECD) presented in its study of 2017, "Enhancing the Role of Insurance in Cyber Risk Management", collected data from Marsh reports where they estimated the rates of acquisition of cyber insurance by sector, based on

its client's information (mostly US clients) (OECD, 2017). Figure 2.3 shows these take up rates by sector of activity.



Source: OECD. (2017). Enhancing the Role of Insurance in Cyber Risk Management.

Figure 2.3. Estimated stand-alone cyber-insurance take-up rates by sector

According to OECD, the stand-alone cyber insurance market reached an estimated 3,5 billion dollars in written premiums in 2016, of which approximately 3 billion dollars was written on behalf of US-based companies and 300 million dollars was written on behalf of European companies (OECD, 2017). Additionally, it is expected that the market continues to grow in Europe mostly due to the implementation of the EU General Data Protection Regulation (GDPR) which will create uniform notification and disclosure requirements.

Insurance industry forecasts predict an expected growth in cyber premiums from around 2 billion dollars in 2015 to some 20 billion dollars or more by 2025, as stated in the study of Woods & Simpson, "Policy measures and cyber insurance: a framework. Journal of Cyber Policy" (Woods & Simpson, 2017).

2.2. MAIN CONSEQUENCES OF CYBER RISK

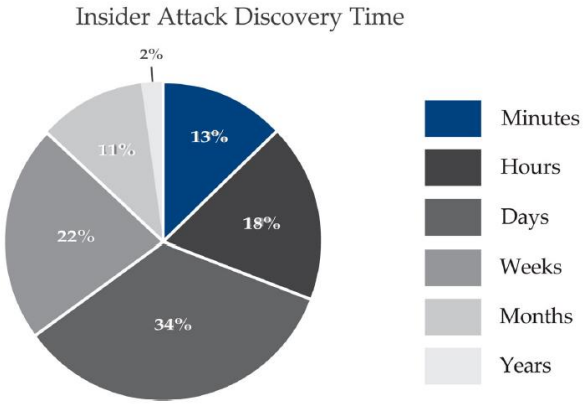
An interesting approach to interpret the frequency and severity of cyber-attacks is the one developed by Delloite in its research "Beneath the surface of a cyberattack", in 2016. It allocates the different consequences of cyber-attacks along the length of an iceberg (Deloitte, 2016).

At the top of the iceberg, and thus surfaced, are those direct consequences of a cyber-attack. They are those that are felt immediately or that impact in short term the normal functioning of the institutions and the integrity and confidentiality of the information. Those have the better-known cyber incident costs like technical investigation, customer breach notification, post-breach customer protection, regulatory compliance, public relations, attorney fees and litigation and cybersecurity improvements.

Beneath the surface will be the hidden or less visible consequences of cyber-attacks. Those may only be known several years after the attack. They are insurance premium increases, increased cost to

raise debt, impact of operational disruption or destruction, lost value of customer relationships, value of lost contract revenue, devaluation of trade name and loss of intellectual property. These costs/consequences are explained in more detail in annex 1.

In fact, there are many ways a cyber-attack can affect an organization, and the impacts will vary depending on the nature, severity of the attack and the time of action after identifying it. According to a study of Camillo, "Cyber risk and the changing role of insurance" in 2017, it was found that in 34% of the cases investigated it took days to discover an insider attack, followed by 22% of the cases that took weeks and 18% took hours, as can be shown in figure 2.4.



Source: Camillo, M. (2017). Cyber risk and the changing role of insurance. Journal of Cyber Policy.

Figure 2.4. Insider attack discovery time

There is more awareness that the first 48 hours following detection of a breach are a critical window of opportunity to contain a crisis, according to Camillo, 2017. Additionally, a further 45 days following discovery of a breach is needed on average for recovery and mitigation. Therefore, it can take up to seven months between the initiation of an attack and recovery from it, with some breaches taking a year or more to resolve (Camillo, 2017).

So, there are just a few consequences that stay "at the iceberg's surface". Most of them remain submerged, which is why it is so difficult to predict the real impacts of a cyber-attack.

2.3. REAL LIFE EXAMPLES

In the past years there was a realization that companies could no longer hope to simply avoid cyber-attacks through IT security. Several cyber incidents demonstrated that even organizations with robust risk mitigation and security measures were not immune.

Historical data prove that no matter the size of the company or the sector that it operates, cyber-attacks are a real threat to everyone.

Annex 2 shows examples of that. Many companies among the most variate sectors, like health, telecommunications, food, energy and business sector suffered from cyber-attacks in the past years.

Additionally, annex 3 shows several cyber incidents affecting the banking sector. According to Banco the Portugal, the institutions of financial sector concentrated more than 25% of all the malicious cyber-attacks in 2018 (Banco de Portugal, 2019).

It should be noted that the information collected represent a very small sample of what cyber-attacks have been over the years. The more exhaustive the search, the more historical records will be found in the years before, during and after the dates presented.

Cyber threats are the new risks of the modern world and it is likely that continue to rise along years as cyber-attackers are becoming more sophisticated and innovations are in constantly development.

2.4. CYBER RISK IN PORTUGAL

Cybercrime threatens Portuguese and global companies. This is a risk in which there is still relatively little experience in Portugal (and even in Europe). However, several studies are being developed.

Lloyd's Iberia find out in its investigation that the immediate exposure of Lisbon economy to a catastrophic risk involving natural phenomena, human action (the case of a cyber-attack) or even a humanitarian crisis is in the order of 1040 million dollars. Of this amount, about 840 million dollars will be human responsibility and the rest will be natural risks. Additionally, they revealed that the five biggest risks that Lisbon faces are the market crash that could involve 550 million dollars; floods with an impact on the city's Gross Domestic Product (GDP) of around 100 million dollars; while a cyber-attack will cost the city 80 million dollars' worth of city's GDP (Bernardo, 2018).

Additionally, the research carried out by Marsh in 2018, "The Portuguese companies' vision of Risk 2016, 2017, 2018", in which 170 Portuguese companies participated, regarding the risks that Portuguese companies considered they could face in 2018, pointed that cyber-attacks were identified as the main risk (with 57%) being at the forefront of risks such as political or social instability and extreme weather events. In 2017 this statistic was only 36%, occupying the second place in the top 5 and in 2016 had only 25% (Marsh, 2018).

According to MDS's presentation entitled "Cyber Risk. Ameaça virtual versus ameaça real", of June 2019, Portugal is the sixth country in the world with the highest number of computers infected by viruses and about 25% of the Portuguese companies were affected by cyber-attacks in the last year (MDS, 2019).

3. STUDY OBJECTIVES

The main goal of this work is to assess the supply of insurance against cyber risk in the banking sector operating in Portugal.

In order to meet the main goal, there are specific objectives important to be addressed such as characterize the knowledge of insurance sector companies on the cyber risk; characterize the perception of the sector on the main exposures and impacts of cyber risk in banking institutions; check the determining factors for the supply to offer cyber insurance as a mean of protection against the risk; characterize the perception of insurance sector companies on the evolution of the cyber insurance market and finally, characterize the perception of supervisor authority on the cyber insurance market and its evolution.

4. LITERATURE REVIEW

4.1. CYBER RISK

4.1.1. Overview on Cyber Risk

There is no standardized definition for cyber risk. Regulators of insurance and financial markets follow the operational risk frameworks stated in Basel II and Solvency II to categorize cyber risk. They define it as an "operational risk to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems" and categorize it into four classes: actions of people, systems and technology failures, failed internal processes and external events (Biener, Eling, & Wirfs, 2014).

The definition adopted by the European Banking sector goes along to that defined by Basel II. They define a security risk as "the risk resulting from inadequate or failed internal processes or external events that have or may have an adverse impact on the availability, integrity, confidentiality of information and communication technology (ICT) systems and/or information used for the provision of payment services. This includes risk from cyber-attacks or inadequate physical security" (EBA, 2017).

Another two possible definitions are summarized in the issuer paper written by International Association of Insurance Supervisors (IAIS), "Issues Paper on Cyber Risk". One arose during a CRO Forum where it was broadly described as "any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information − be it related to individuals, companies, or governments." The other one arose from the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions that described it as "the combination of the probability of an event occurring within the realm of an organization's information assets, computer and communication resources and the consequences of that event for an organization" (IAIS, 2016).

Principals like confidentiality, integrity, and availability of companies' data are therefore an essential part of cyber risk's definition and prevention. In annex 4 is presented the conceptual definition of those principals, developed by sources like IMF[4] and IRM[5] in those works created in 2014 and 2018 respectively.

The classification of cyber risk can also depend on the context. There are two possible contexts to consider: the demand side (companies buying cyber insurance) and the supply side (insurance companies selling cyber protection).

For buyers, cyber risk can be interpreted as an operational risk. For insurance companies, however, the allocation of cyber risk depends on which part of the business is considered. If it is considered insurance companies as providers of insurance coverage, then cyber risk is an insurance risk. If,

[4] IMF, & Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.

[5] IRM. (2014). Cyber Risk: Resources for Practitioners.

however, it is considered an insurer as a company that can be hacked and seeking for protection against cyber risk it is interpreted as operational risk (Eling & Wirfs, 2016).

4.1.2. Categories and Subcategories of Cyber Risk

In the study of Biener, Eling, & Wirfs, "Insurability of Cyber Risk: an empirical analysis" in 2015, they refer three criteria that an event must fulfill in order to be categorized as a cyber risk:

1) A critical asset such as a company server or a database needs to be affected;
2) A relevant actor needs to be involved in the cause of the cyber risk incident (e.g., hackers, employees, system, and nature);
3) A relevant consequence needs to be present, such as a loss of data or misuse of confidential data.

Many categories of cyber risk as well as their subcategories have already been identified in several studies. The Cebula and Young approach ("A Taxonomy of Operational Cyber" in 2010) is widely accepted and used in this kind of research work. They divided cyber risk in four main categories. They are actions of people, systems and technology failures, failed internal processes and external events. Those categories fulfill the three criteria stated above. They satisfy criteria (1) once in all of them a company server or a database is affected, criteria (2) once each of them has a source of cyber risk and criteria (3) because all categories have consequences, some more serious than others, for the organizations. So, all the categories and subcategories presented by Cebula and Young are considered as cyber risk according to the Biener, Eling, & Wirfs criterion.

Beyond this categorization, a possible classification can be attributed to the categories and subcategories of cyber risk. This classification is presented by Eling & Wirfs, in their work "Cyber Risk - Too Big to Insure?" in 2016, where they propose a distinction between criminal or non-criminal sources of cyber risk. Annex 5 shows those classification and give examples to each of them.

In annex 6, it is presented an aggregation of the main categories and subcategories of the cyber risk proposed by Cebula and Young with the classification presented by Eling & Wirfs in their study.

The research carried out by Biener, Eling, & Wirfs verified that actions of people are considered the main source of cyber risk while the other categories, such as external disasters, are very rare. Mark Camillo, for the Journal of Cyber Policy, also reinforce that "a significant number of successful cyber intrusions have a human element" (Camillo, 2017). In this way, privileged users, that have access to an organization's network, devices and servers, are often an organizations' greatest security risk.

So, there are several types of cyber incidents that fill in the categories described above. In most of the times it is difficult to detect the source, infer the damages and losses and find out the potential ways to avoid other incidents. Annex 7 present a wide list of cyber incidents. There isn´t a standard and static labeling of cyber risk events since the nature of this risk is very dynamic and it is in increasing sophistication. The intention is not to present a 'definitive' overview of all types of incidents, but simply to give an idea of the most common types. It is an aggregation of several cyber incidents stated by numerous authors.

4.2. CYBER INSURANCE

4.2.1. Overview on Cyber Insurance

Several companies regardless of size and sector collect, store, and share substantial amounts of private and confidential information with various third parties, may they be service providers, intermediaries, costumers or insurers.

The usual approach to managing information security risk is like other business risks. Ideally it is intended to eliminate the sources of risk, then mitigate them, absorb and, if possible, transfer.

Since cyber risk cannot be totally eliminated because of its dynamic and ever-changing nature, companies can adopt several options of risk response as: risk avoidance (for example, avoid use of USB flash drives); risk mitigation (control objectives and control measures like protection technologies (firewall, antivirus, encryption) and security procedures (passwords security, access control)); risk transfer (cyber risk insurance) and risk acceptance (self-insurance) (Kosub, 2015).

There are several risk transfers options possible to an organization to adopt. They differ from each other by the agent that take the risk. A study developed by Martin Eling and Jan Hendrik Wirfs from University of St. Gallen in 2016, stated several forms of transferring risk. It can be through a risk pool, insurance, reinsurance, capital markets or governments. Annex 8 shows a summary of risk transfer possibilities available.

In the case of buying insurance as a transfer of risk option, an insurance contract (policy) binds an insurance company (supply side) in the occurrence of contractually defined loss events to pay a specified amount (claim) to the insurance holder (demand side). In return, the insurance holder pays a fixed sum (premium) to the insurance company to receive financial compensation in case of certain IT related adverse event occurs (Franke, 2017).

The process of underwriting a cyber insurance is very specific from company to company. Even in the same industry differences may exist in the way that companies use, process or store their information so there are variances related to the selection of the coverage type and to the risk assessment phase of security and cyber protection, where the evaluation of the security systems and tools by IT specialist and insurer is done. That assessment can influence sometimes the amount of the premium that is calculated (ENISA, 2012).

Cyber insurance seems to be a solution each more adopted by companies to transfer their risk exposure. According to a study done by European Insurance and Occupational Pensions Authority (EIOPA) in 2018, “the increasing number of cyber incidents, the continued digital transformation and new regulatory initiatives in the EU are all expected to raise awareness and boost the demand for cyber insurance” and “the growth in the cyber insurance market is a sure sign of firms’ increasing awareness of cyber risk and appetite to transfer exposure”. In fact some markets are already more aware of this new emerging risk than others that is the case of the US market where cyber insurance is frequently regarded as an “hygiene factor” (Franke, 2017) meaning that it is seen as part of a necessary security pack that all businesses should have.

4.2.2. Coverages and exclusions

Cyber insurance coverage

As stated above, risks faced by corporations are often unique to its industry or even to the company itself, so most undertakings provide tailor-made solutions. Company size, size of the customer base, web presence, and type of data collected and stored are important determinants of cyber insurance policy terms and pricing (Biener, Eling, & Wirfs, 2015).

The significant property that distinguishes cyber risk from conventional risk is that ICT resources are interconnected in a network, and therefore the analysis of risk and its related potential losses needs to take into account the network topology (Xu, Hua, & ASA, 2017).

Cyber insurance can provide coverage for both first party and third-party liabilities. First party risks are the ones that directly affect the insured. Third party risk are risks that might initially affect someone other than the insured (first party) or insurer (second party, against which an insured like to have coverage (ENISA, 2016).

In annex 9, can be seen the common coverages from first-party and third-party losses, outlined by EIOPA in its study "Understanding cyber insurance" of 2018.

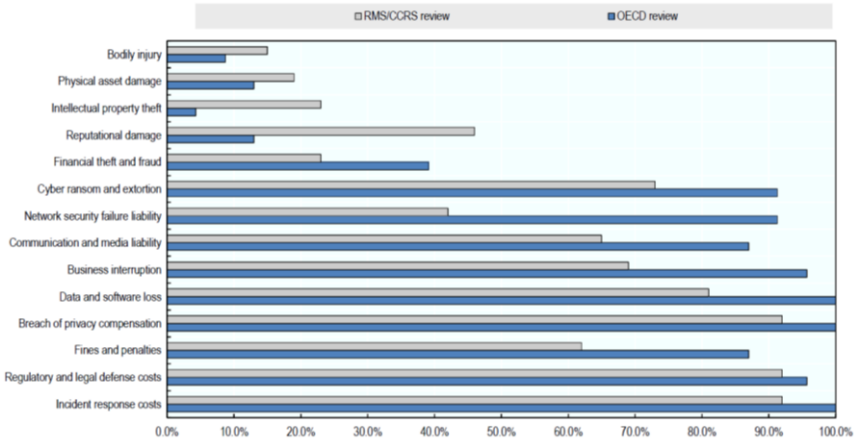
Additionally, cyber insurance can be offered in three different ways: 1) a stand-alone product, 2) a specific endorsement on existing policies (an add-on coverage to traditional lines of business) or 3) as part of traditional coverages without a specific endorsement (often referred to as silent cyber coverage that refers to cases where cyber exposure is neither explicitly included nor excluded within an insurance policy) (EIOPA, 2018) (OECD, 2017).

1) Stand-alone cyber insurance policies

The stand-alone cyber insurance market was developed in response to the introduction of exclusions of cyber-related losses like property, crime, kidnap and ransom. OECD has presented in its study, "Enhancing the Role of Insurance in Cyber Risk Management", which exclusions may exist: (i) general exclusions of all losses resulting from a cyber-attack or incident; (ii) an exclusion applied in general liability policies to exclude liability related to data breaches; and (iii) exclusion of losses related to data restoration (OECD, 2017).

The coverage provided by stand-alone cyber insurance policies can vary significantly across providers. The abundance of policy forms may be partly due to the common practice of offering a menu of possible coverage options allowing policyholders to tailor their policy terms based on their specific level of exposure (OECD, 2017).

OECD presented also an overview of the possible coverage for different categories of cyber-related losses. This overview was based on responses to the OECD questionnaire as well as on its review of selected publicly available descriptions of policies from major providers (total of 23 providers based in 7 countries). For comparison, it also shown the results of a similar exercise undertaken by Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies in 2016 of 26 stand-alone policies. Figure 4.1 shows the results of most commonly losses covered under a stand-alone policy.



Source: OECD. (2017). Enhancing the Role of Insurance in Cyber Risk Management.

Figure 4.1 Loss categories commonly included in stand-alone policies

As the graph suggests the more commonly coverage loss categories, representing more than 50% are the incident response costs, regulatory and legal defense costs, fines and penalties, breach of privacy compensation (that represent the data confidentiality breaches); business interruption losses; network security failure liabilities, data and software loss, cyber ransom and extortion losses and communication and media liability.

In the case of fines and penalties, some policies will not cover it or will only provide such coverage where permissible by law. Another case is of cyber ransom and extortion where there is some variation in the types of losses covered. Some providers only cover costs related to efforts to avoid paying a ransom, not the payment of a ransom itself. Insurance companies may also choose not to provide such coverage in order to be consistent with government policies that are explicitly opposed to making ransom payments in response to kidnapping/extortion.

The other categories are not so commonly covered, according to OECD data. In some cases because it is a challenge for insurers to quantify the possible losses and impacts and, in the case of financial theft and fraud, the low level of coverage may be because many traditional crime policies provide coverage for financial theft without any exclusion of cyber-related incidents (OECD, 2017).

Stand-alone cyber insurance products generally include additional services such as the access to service providers that can assist policyholders in responding to cyber incidents and preparing response plans (Marsh & McLENNAN, 2018). Some insurance companies provide first response incident management as an integrated part of their products. These services not only help companies to improve their security structure but also give insurance companies a degree of control of the quality of incident management, making it easier to predict and manage the costs of incidents. However, in most cases the insurance companies do not provide this service in-house, but rather partner with IT consultancies, law firms or consultants who deliver the actual first response services (Franke, 2017).

2) and 3) Cyber risk coverage in traditional insurance policies (endorsed and silent)

Some insurance coverage for losses resulting from cyber incidents may be explicitly (endorsed) or implicitly (silent) covered in traditional policies as is the case of property, general liability, Directors and Officers liability, errors and omissions liability/professional indemnity, crime/fidelity, kidnap and ransom policies.

As organizations assess their cyber insurance coverage options, it is important to understand how cyber incidents may be covered in existing policies. This is a challenge for many organizations as there can be overlaps or "silent coverage" for cyber incidents in existing policies (Marsh & McLENNAN, 2018).

According to OECD, the most common coverages for cyber risk in traditional policies are (OECD, 2017):

- Property policies – data and software loss, business interruption, physical damage;
- Liability policies – Incident response costs (compulsory investigations), regulatory and legal defense costs, fines and penalties, breach of privacy compensation, network security failure, communication and media liability, product liability, directors' and officers' liability, professional indemnity;
- Crime/fidelity policies – financial theft and/or fraud;
- Kidnap and ransom policies – cyber ransom and extortion.

In insurance companies' point of view there are some challenges regarding coverage. According to OECD there are significant losses from cyber incidents that are not usually included within the scope of stand-alone or traditional insurance coverage like the impacts on a company's reputation and future business and the loss of value of intellectual property. In both cases, the key impediment to coverage is the difficulty in quantifying the value of the future business that has been lost due to reputational damage or the reduced ability to exploit the commercial value of intellectual property (OECD, 2017).

Besides that, insurers typically impose a maximum loss limit for cyber risk policies in order to protect themselves against unexpected amounts of exposure. This cover limits can vary between insurance companies and whether this amount is acceptable depends on the risk preferences and cyber risk exposure of the individual policyholder. An increase in coverage should be negotiable but will result in higher premiums.

Another severe problem regarding cover limits is policy complexity. According to Biener, Eling, & Wirfs, the dynamic nature of cyber risk and the existence of several exclusions in cyber insurance contracts rises the uncertainty about what the cyber policy covers for the seller and the buyer (Biener, Eling, & Wirfs, 2015).

Cyber risk exclusions

Insurance companies make exclusions in their insurance contracts also in a way to protect themselves against unexpected risk that they are not willing to accept from the client (Franke, 2017).

Once insurers are increasingly excluding cyber coverage under existing policies it places a growing focus on the need and value of standalone policies (Marsh & McLENNAN, 2018).

EIOPA presented in its study, "Understanding Cyber Insurance: a structured dialogue with insurance companies" in 2018, the main exclusions reported by the participant companies (13 (re)insurance groups based in Switzerland, France, Italy, Germany and UK): war, political risks, nuclear, (cyber) terrorist attacks, property and material damages, bodily injury, unauthorized collection of data by the insured, strike, infrastructure failure, theft of telecommunications services, online gambling, large online consumer auctions, payday loan companies, non-malicious cyber, natural perils, contingent business interruption (CBI), directors and officer (D&O) warranties, claims from internet service providers, regulatory fines, economic value of data, extortion payments, adult entertainment, online and offline dating agents, online sales of firearms, virtual currencies (EIOPA, 2018).

The research of Franke, "The cyber insurance market in Sweden" in 2017, stated also another two possible exclusions that fits to modern concerns. One of them is the offering to cover internal outages and outages at external service providers. Some companies do not make any distinction between internal or external service providers, but others may have restrictions allowing coverage only to a specific list of providers (Franke, 2017). The other one is the coverage offered for subsidiaries and corporate entities in different jurisdictions (Franke, 2017).

Also, legal restrictions might prevent certain coverage for cyber insurance. For example, in many countries, insuring against regulatory fines is prohibited (Biener, Eling, & Wirfs, 2015).

4.2.3. Requirements and controls

Requirements and controls on the insured – Supply Side

In the supply side, some insurers have a basic criterion that need to be fulfilled by costumers in order to get a cyber insurance offer. As stated above, insurance companies are not willing to insure any risks. A study done by Ulrik Franke, "The cyber insurance market in Sweden", stated that insurers offers can vary from none, partial or total protection, depending on the outcome of a customer's risk assessment (Franke, 2017).

Nowadays insurance companies not only require knowing but might also validate a customers' preparation level and assist them by offering consulting, cyber risk assessment or incident response services (ENISA, 2016).

The process of assessing the costumer's exposure to risk vary from company to company. According to AIR study, "Insuring Cyber risk" in 2017, there are several ways of assessing a costumer or a potential one cyber risk's exposure. It can be, for example, through self-assessment questionnaires

to costumers, additional reports developed in-house by cyber risk engineers, externally resources provided by specialized consultancies such as auditors and IT security consultants (who may perform e.g. penetration tests), letting the procedure depend on the costumer or through interviews with stakeholders such as Chief Information Officer (CIO), Chief Financial Officer (CFO), Chief Executive Officer (CEO) (AIR, 2017). Insurers become a 'de facto regulator' by establishing a minimum-security level to gain cyber coverage (Woods & Simpson, 2017). So, cyber risk assessment is a way for insurance companies to control the risk they are taken in but also gives opportunity to customers increase awareness of cyber risk exposure, potentially increasing self-protective efforts and maybe get a lower premium (Franke, 2017).

ENISA stated in its study, "Cyber insurance: recent advances, good practices and challenges" in 2016, that when assessing a clients' risk, insurers generally focus on the following main categories (ENISA, 2016):

- Dedicated Resources – validate the presence of leadership roles with Information Security focus; the number of employees that are dedicated to Information Security; the time allocation to tasks other than what their role mandates and the reporting lines of a Chief Information Security Officer (CISO);
- Policies and Procedures - validate the existence of an Information Security program (covers technical, administrative and physical measures for data protection);
- Employee Awareness – validate the presence of a formal Security Awareness program, which is a key element for safeguarding the human factor within a company. Top management, brand managers, social media page administrators and all the other employees should have regular and tailored training on how to implement, monitor and enforce the guidelines that the policy has set out;
- Incident Response – validate the existence of an Incident Response program. It defines the processes and resources that an organization engages for addressing any Information Security incidents. Response plans should include preliminary drafts of communications to all stakeholders including customers, suppliers, regulators, employees, the board, shareholders, and even the general public. The plan should also consider legal requirements around timelines to report breaches.
- Security Measures - confirm the proper implementation of Business Continuity Planning, data classification, data retention, access control, log monitoring, intrusion detection, network segmentation, network monitoring, vulnerability management (ENISA, 2016), penetration testing and scanning of systems (EIOPA, 2018).

Additionally, and according to the same source, under the questionnaires applied to several European insurers, they pointed as a good security measure the compliance with some Cyber Security Standards such as: Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), ISO 27000 family, Payment Card Industry Data Security Standard (PCI-DSS) and Sarbanes-Oxley (SOX) Act.

Requirements and controls of the insured – Demand Side

On the demand side, organizations should ask if they are making the appropriate investments in security, vigilance, and resilience, and whether those decisions are based on a realistic understanding of the specific risks their organization faces as well as the magnitude of impact that a cyber-attack could have (RSA, 2016).

Insureds will need to demonstrate that they fulfill certain "cyber hygiene" and pre-loss standards in order to obtain indemnification. To be effective, cybersecurity needs to be addressed at all levels of an institution and with respect to relevant third-party arrangements (IAIS, 2016).

It is very unlikely and most probably impossible to prevent all cyber losses due to the ever-growing frequency and complexity of the criminal efforts to steal data. Indeed, in some areas the cost to mitigate the risk may be many times more than the actual loss of that piece of data. It is however essential to implement controls which can help minimize the potential impact to the organization (IRM, 2014).

If a company can show that it has adopted a set of practices generally considered to be worthwhile things to do with respect to cyber-security, then this will reduce information asymmetries and better demonstrate to the market that the firm takes security seriously. This feeds into premiums once if an insurer can observe that a firm is undertaking various 'effective' security measures, then the premium will be reduced on the basis that the firm is less prone to risks (ENISA, 2012).

Advantages to invest cybersecurity:

Deloitte Advisory Cyber Risk Services stated, in RSA study "Cyber risk appetite: Defining and Understanding Risk in the Modern Enterprise", that "managing cyber risk is not just a cost to the business, but a positive investment to enable the success of strategic growth and performance initiatives" (RSA, 2016). In fact, there are several advantages in choosing to invest in cybersecurity. The points below show the risk mitigation main advantages recognized by several sources:

- Improved business performance;
- Competitive advantage through a stronger customer value proposition;
- Greater organizational awareness of cyber risk and its potential impact on the business. The process of seeking insurance coverage requires policyholders to understand (and quantify) the risk that they face in order to determine the amount of coverage that they require (OECD, 2017);
- Internal transparency on cyber risks and controls in place. Generating an organization-wide approach to ongoing cyber risk management by all aspects of the organization (EIOPA, 2018);
- Assessing the strength of cyber defenses, particularly among a rapidly changing cyber environment (EIOPA, 2018);

- Clear compliance with external regulatory controls. The underwriting process will usually involve an assessment of risk management and security practices, including recommendations on further preventative measures that could be taken (OECD, 2017);
- Incentives for firms to increase IT security in order to reduce premiums (ENISA, 2012).
- Demonstrate strong business practices to investors (ENISA, 2012);
- Incentives and means to promulgate best practices (ENISA, 2012).

4.2.4. Underdevelopment causes

As stated above, cyber insurance is gaining field as a good measure to manage cyber risk, but some aspects hold it back.

Camillo stated in his study, "Cyber risk and the changing role of insurance", that during the late 1990s and early 2000s, companies focused mainly in loss mitigation through network security and, in that time and still nowadays, cyber insurance market remains a niche area, lacking the scope and capacity once a cyber insurance product remains untested and there are a lack of historical loss data. Furthermore, EIOPA in its paper, "Understanding cyber insurance" in 2018, concluded that "there is a clear need for a deeper understanding of cyber risk, both on the supply and demand side, for the European cyber insurance industry to develop further. This relates not only to the assessment and treatment of risks in new cyber insurance propositions, but also to the understanding of clients' own needs" (EIOPA, 2018).

It will be described below a gathering, collected from different sources, of the main causes for cyber insurance market underdevelopment and the challenges felt by supply and demand:

Insurers – Supply side

- The information asymmetries inherent in cyber risk: moral hazard and adverse selection. They are the most widely spoken causes for the underdevelopment of cyber insurance market. In the adverse selection problem, the insurer cannot discriminate different types of customer before a contract is signed and therefore price the premium accordingly (ENISA, 2012). Besides that, firms that have experienced a cyber-attack are more likely to purchase insurance resulting in adverse selection once a firm may apply for cyber insurance in the knowledge that they are relatively more exposed to cyber risk. In the moral hazard problem, the insured, once a contract is signed, may be incentivized to behave more insecurely in the knowledge that the insurer will bear some of the loss (Biener, Eling, & Wirfs, 2015);
- The perception of effectiveness of various types of cyber-security measures implemented by costumers. It is essential for the process of offering a cyber insurance product that the insurance company knows exactly the extension of risk that the costumer is exposed to in order to accept or refuse to take that risk. Sometimes that process is not so much transparent (ENISA, 2012);

- The misevaluation of accumulation risk. Cyber risk is not an isolated threat. There are several potential correlated exposures to this risk that are very difficult to predict and to estimate their probable losses. These correlations can be present through third party, outsourcing exposures or through non-affirmative risks or "silent" risks[6]. It is a challenge for insurance companies to be certain about the number of customers that would be affected. Many insurers set relatively low limits and a multitude of exclusions to try to control their potential losses, in addition to high premiums. The potential for accumulation risks may discourage some insurers and reinsurers from entering the cyber insurance market at all (EIOPA, 2018);
- Lack of government intervention as 'insurer of last resort' may inhibit cyber insurance supply (ENISA, 2012);
- The ever-changing form of cyber threats. This causes that a control measure that may have been effective a year ago may now prove to be a vulnerability. Technology innovations drives fluctuations in risk and threats that makes it difficult (from an actuarial perspective) to forecast future losses from past events and utilizing predictive analytics for the assessment of potential risks and impacts (IRM, 2014);
- Lack of commonality in risk assessment language - there is not an implemented standardized linguistic among institutions (ENISA, 2017);
- Lack of specialized underwriters, robust actuarial data and quantitative tools (EIOPA, 2018) (OECD, 2018). The absence of relevant data series on past losses, the limited actuarial information available on the frequency and size of actual and potential cyber security incidents and the lack of stochastic models are key obstacles preventing insurers from developing the predictive models they depend on to set accurate premiums, exposure models and the provision of proper coverage;
- Reduced willingness of insurance companies to extend significant amounts of coverage. The topic is the main responsible to this reduction and leads to cyber insurance offers with several exclusions and sub-limits that customers may find unappealing (EIOPA, 2018) (OECD, 2018).

[6] Non-affirmative risks or "silent" risks – ""Silent cyber", also known as "unintended" or "non-affirmative" cyber, refers to the unknown or unquantified exposures originating from cyber perils that may trigger traditional property and liability insurance policies" (Carpenter, 2018). To see more about that topic: http://www.guycarp.com/content/dam/guycarp/en/cmp/Affirm%20vs%20Silent%20Cyber%20Briefing%20FINAL%20(2).pdf

Companies – Demand Side

- The absence of clarity on coverage, policy terms and conditions - The lack of similar terminology and different approaches to offering coverage, along with the complexity of the policies themselves, add to the frustration and reduce buyer demand (EIOPA, 2018);
- The lack of understanding by clients of their own risks - Many companies believed that they have nothing a cyber adversary would seek for or they only start to be aware of that threat from the day they are attacked (EIOPA, 2018);
- The perception that existing insurance already covers cyber-risks - Some companies already think that they are insured under existing traditional policies, so they are discouraged from taking out specific cyber-insurance policies on the basis of a fear of being over-insured (EIOPA, 2018);
- The reputational implications of sharing information - some companies fear in sharing information under a full transparency and non-anonymized approach. This would prevent the collection of data, the spread of good practices among companies and consequently the development of the sector (EIOPA, 2018);
- The premiums charged for cyber insurance coverage are high and variable - Given the large tail risks and uncertainties around cyber risk, cyber insurance is currently relatively expensive compared to other types of insurance coverage, with estimations that can be three times more expensive than general liability coverage and six times more expensive than property insurance This became cyber insurance market unattractive for companies. (EIOPA, 2018).

For that main challenges faced by the cyber insurance market are already possible solutions. In the study developed by EIOPA, they stated some of those possibilities such as insurers could introduce explanatory sessions to their customers to provide understanding about their potential exposures to cyber risk and provide customer scenarios and generic examples of policy coverage once could act as a fast method to raise awareness and understanding of cyber insurance; they could also make a review of the wording in contracts in order to clarify the policy language and avoid using generic terminology that can be interpreted in multiple ways; they could also offer a transparent underwriting process, detailing the criteria and criticality that drives pricing and develop a Risk Assessment Guidelines in order to facilitate the analysis of their costumers exposure to risk.

In the costumers side, ENISA stated in its study, “Cyber Insurance: recent advances, good practices and challenges” developed in 2016, that organizations should get informed, prepared, and document their environment, before requesting a cyber insurance policy possibly by attending in explanatory sessions or provide specialized training to employees and nominate a CISO for companies in order to institutionalize the culture of cyber risk management in the organization structure.

Eling&Wirfs stated in their study, “Cyber Risk: Too Big to Insure?”, possible top five measures to improve insurability of cyber risk and hence help to develop the market. They are to incentivize the development of an anonymized data pool; develop minimal standards for risk mitigation; introduce

reporting obligations; incentivize the development of "traditional" risk transfer mechanisms and establish a governmental backstop for extreme scenarios (Eling & Wirfs, 2016).

Additionally, general initiatives in terms of legislation and government intervention can also improve significantly the development of the market. A study of Daniel Woods and Andrew Simpson, "Policy measures and cyber insurance: a framework" in 2017, stated that "insurance industry should be more involved in the Cyber Security Information-Sharing Partnership (CISP), which enables government and industry to share information". They believe that one of the major ways of managing cyber risks is through appropriate sharing of technical information and data.

Government intervention

Governments can potentially play a role in supporting the development of the market and maximizing the contribution it makes to manage this fast-evolving risk. However, this is a field that need to be developed.

The study done by Elling&Wirfs, pointed out in its main conclusions that "cyber risks "of daily life" are not too big to insure" but on the other hand, ""extreme scenarios" (e.g., a breakdown of the critical infrastructure for a period long enough to impact the economy (EIOPA, 2018)) are difficult to insure." They propose that insurability for those "extreme scenarios" could be improved by "integrating the government in various ways." In the same study they structured possible means of governmental intervention (Eling & Wirfs, 2016). They are presented in annex 10 of this work.

Sharing the same opinion, EIOPA under their paper "Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies" in 2018, stated that government intervention might be needed in case of extreme events. Once cyber risk has a great potential for significant accumulation of losses and it is difficult to estimate the extent of major cyber incidents, the government is often seen as a potential last resort of the system.

4.3. CYBERSECURITY IN BANKING SECTOR

A bank runs multiple servers that store enormous amount of information and details of various operations such as credit cards, real time gross settlements, ATMs and SWIFT and others. Financial institutions adopt digital channels like online banking and mobile banking to increase access and provide convenience to customers but at the same time it grows the attack surface once it opens the door to online security risks (Reddy & Bhargavi, 2018).

According to Reddy and Bhargavi study, "Cyber security attacks in banking sector: Emerging security challenges and threats" in 2018, cybersecurity attacks increased in the banking industry during 2016 and they have not shown any signs of abating. The risks are prevalent across all areas of the sector affecting large and small banks. Banking institutions are considered a gainful target for cybercrime once they are a source where the money and important information is (Reddy & Bhargavi, 2018).

In the European Banking Authority (EBA) semi-annual Risk Assessment Questionnaires (RAQs) among 53 European banks and 15 market analysts, carried out in 2018, it was concluded that more than 50% of banks expected an increase in operational risk in their institution. The main driver identified by

banks was cyber risk and data security (around 90%). Around 55% of market analysts saw an increase in EU banks' operational risk, mainly driven by legal risk, cyber risk and data security (both agreed by 90% of respondents), followed by IT failures (65%) (EBA, 2018). This reinforces the idea of a growing trend of cyber-attacks occurrence in the sector.

Cyber-attacks to banks can take many forms. Commonly the attackers are seeking to acquire capital as well as confidential data and sensitive information. According to, Reddy and Bhargavi, based on the number of recent attacks, they estimate that many banks are not mature and prepared to deal with this kind of threats and need to address their financial-crime security efforts across the board (Reddy & Bhargavi, 2018). The cyber security attacks most common on banks, according to the author are phishing, cross site scripting, vishing, cyber-squatting, bot networks, malware, denial-of-service (DoS) attack, SMS tricking, Internet Protocol (IP) spoofing, pharming, insider threats, SMS One Time Password (OTP) attacks. More details about these cyber threats are shown in annex 7 of this work.

Many statistics can also be found on the most common types of cyberattacks in financial and insurance services. Although differences can be observed in these statistics across research sources, there is a broad consensus that DoS, web application attacks and payment card skimming represent many security incidents. The most common purpose for these attacks is financial, whereas a small share is driven by espionage and other purposes. For the vast majority of cyberattacks, the compromised data are credentials (CEPS & ECRI, 2018).

Cyber events can disrupt financial services and undermine the security and confidence of the financial system (Institute of International Finance, 2018). If the attack is large enough it could even lead to the disruption of the global financial system and on overall financial stability (Institute of International Finance, 2018).

According to Banco the Portugal study, the main risks associated to cybersecurity incidents in banking sector are financial risk, reputational risk, operational risk and legal risk (Banco de Portugal, 2019). The annex 11 shows several examples of those risks.

4.4. LEGISLATION IN FINANCIAL SECTOR - OVERVIEW

Authorities around the world have developed strategic initiatives, guidance papers, regulatory and supervisory approaches aiming to strengthen the cyber-resilience of both individual institutions and the global financial system (Institute of International Finance, 2018).

It is evident that regions with established cybersecurity-related legislation, have a higher cyber insurance adoption than regions that have recent or no formed legislation. The expected growth for the European market is anticipated to be further accelerated by the adoption of the GDPR and NIS directive (ENISA, 2016).

According to a study done by EIOPA, "*Understanding Cyber Insurance: a structured dialogue with insurance companies"* in 2018, they collect that the predominant view of the study's respondents was that the expected increase in demand for cyber insurance will be more gradual rather than abrupt. Reasons for this are that it is yet unclear whether GDPR fines and fees will be insurable and

the fact that the new regulation is very extensive, with most companies focusing on compliance for now. However, it is expected that GDPR will ultimately increase awareness of cyber risk and stimulate demand for cyber insurance (EIOPA, 2018).

Regulatory changes are found to impact cyber insurance to a great extent. Whether these have the form of mandatory notification, introduction of fines, or “right to know” for users – they ultimately result in a better market preparation, of which cyber insurance is a part of (ENISA, 2016).

Regulation may be welcomed by the industry in a moderate fashion, as it could help to address some of the identified challenges notwithstanding the need for compliance with the Solvency II-Directive (2009/138/EU) (EIOPA, 2018). Some participants in EIOPA study raised the importance of harmonization of a potential supervisory framework across countries. In that context, an additional area for follow-up work for EIOPA would be to investigate the possibility of introducing (a) new line-of-business code(s) in Solvency II, which could help provide more insights into the quantitative dimension of cyber insurance (EIOPA, 2018).

One of the key challenges for the insurance sector will be to adjust to the increase in demand following the new regulation and the changing customer needs and risk profiles (EIOPA, 2018).

EIOPA suggested some potential contributions of regulation for market development. They are (EIOPA, 2018):

- Ensure appropriate pricing and monitoring of the risks, including potential aggregation risks;
- Ensure incident reporting and exchange of information;
- Regulatory practices envisioning better understanding of risks;
- Introduction of minimum IT and Information security standards;
- Enhance the level of awareness and prudence of new entrants;
- Adequate capital requirements against underwriting risks;
- Avoidance of contagion in case of bigger scale events;
- Ensure adequate estimation of value for money measures;
- Ensure greater clarity about coverage being offered.

5. METHODOLOGY

In order to recognize the supply of cyber risk insurance in the banking sector operating in Portugal, this work will consist on a literature review and an empirical study.

The literature review aims to convey the "state of the art" of cyber risk insurance market and comprises an overview of cyber risk, its main sources and types of cyber incidents; an overview of cyber insurance, the most common covers and exclusions of a cyber insurance contracts and an overview of the cyber insurance market for banking sector, including the most common cyber incidents that banks are exposed.

In turn, the empirical study aims, through the practical application of online questionnaires, to verify the perception of insurers (the sellers or potential sellers) of this risk and their willingness to sell this insurance product. There will be two questionnaires applied to each of the market participants:

- National or international insurers operating in Portugal that sell or not insurance against cyber risk: the department to be questioned varies according to the structure of the insurer. The main purpose is to be applied to the department that developed or could develop the insurance product (production, underwriting or other specific direction);
- Supervisory Authority (ASF).

The study under analysis aims to assess the knowledge and development of Portuguese insurance market in relation to the offer of cyber insurance. For the purpose of work feasibility, the area of study was restricted for the specific case in which the client seeking for that product is a banking institution. So, the questionnaires applied had some general questions but other intended to catch the situation were the offer is specific for a bank.

The various questions that constitutes these surveys, as well as the respective options of answer, were based on this work's literature review.

It is a type of explanatory study whose statistical analysis will be carried out through excel.

The data collection will comprise the period from June 2019 to January 2020.

The questionnaires are anonymous, in order to safeguard the participants' data and the results obtained will be used only for academic purposes.

The questionnaire is divided into four parts: A) General information of the company, B) Knowledge of cyber risk, C) Cyber risk insurance and D) Perception of cyber risk's market evolution. Annexes 12 and 13 show the questionnaires structure and the literature review sources from which the questions were developed.

The table below associates the several chapters and subchapters of the literature review with the research questions applied to insurers.

Research questions applied to insures	Chapter/subchapter of Literature review
A. General information of the company	-
B. Knowledge of cyber risk	**Chapters/Subchapters:** 4.1.2. Categories and Subcategories of Cyber Risk; 4.2.2. Coverages and exclusions **Main articles:** ENISA. (2016). Cyber Insurance: recent advances, good practices and challenges. Cebula, & Young. (2010). A Taxonomy of Operational Cyber. OECD. (2018). Enhancing the role of insurance in cyber risk management. The cyber insurance market: Responding to a risk with few boundaries. Marsh, & McLENNAN. (2018). Cyber Risk Management. Response and Recovery. EIOPA. (2018). Understanding Cyber Insurance: a structured dialogue with insurance companies.
C. Cyber risk insurance	**Chapters/Subchapters:** 4.2.2. Coverages and exclusions; 4.2.3. Requirements and Controls; 4.2.4. Underdevelopment causes **Main articles:** EIOPA. (2018). Understanding Cyber Insurance: a structured dialogue with insurance companies. OECD. (2017). Enhancing the Role of Insurance in Cyber Risk Management. ENISA. (2016). Cyber Insurance: recent advances, good practices and challenges. OECD. (2017). Supporting an Effective Cyber Insurance Market. OECD Report for the G7 Presidency. Marsh, & McLENNAN. (2018). Cyber Risk Management. Response and Recovery. Franke, U. (2017). The cyber insurance market in Sweden. Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: an empirical analysis. ENISA. (2012). Incentives and barriers of the cyber insurance market in Europe. AIR. (2017). Insuring Cyber Risk. What is holding cyber insurance back, and how can the industry push forward? Marsh. (2018). Governing Cyber Risk. A guide for company boards. TheCityUK. Camillo, M. (2017). Cyber risk and the changing role of insurance. Journal of Cyber Policy.

	Eling, M., & Wirfs, J. H. (2016). Cyber Risk - Too Big to Insure?
D. Perceived market evolution for cyber risk	**Chapters/Subchapters:** 4.2.4. Underdevelopment causes; 4.3. Cybersecurity in Banking Sector; 4.4. Legislation in Financial Sector - Overview **Main articles:** EIOPA. (2018). Understanding Cyber Insurance: a structured dialogue with insurance companies. ESA. (2019). Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector. Eling, M., & Wirfs, J. H. (2016). Cyber Risk - Too Big to Insure?

Table 5.1 Research questions by chapter/subchapter and article

6. RESULTS AND DISCUSSION

In order to make both the observation of the results and its discussion more understandable, this next chapter is divided into the four parts that make up the questionnaire applied to insurers. In its conclusion there will be presented the answers to the survey applied to the ASF.

A. General information of the company

The empirical analysis was based on an online questionnaire that targeted insurance companies operating in Portugal, of national or foreign origin, selling or not insurance against cyber risk. Responses were obtained from 9 insurance companies, 4 of which were of national origin.

B. Knowledge of cyber risk

The majority of the participants, more specifically 5 of them, stated having basic knowledge regarding cyber risk. There was only one that stated having advanced knowledge on the topic. The other three felt they had only limited knowledge.

One of the questions asked to the participants was centered on knowing what they considered to be the main sources of cyber risk a bank would be exposed to. Most participants considered the action of people as the main source of cyber risk, as illustrated in Figure 6.1. In fact, the literature review presented above confirms this perception. The action of people is indicated as one of the main sources of cyber risk for companies. This source is essentially composed by employees of the institutions and can be deliberate, inadvertent or inactive actions.

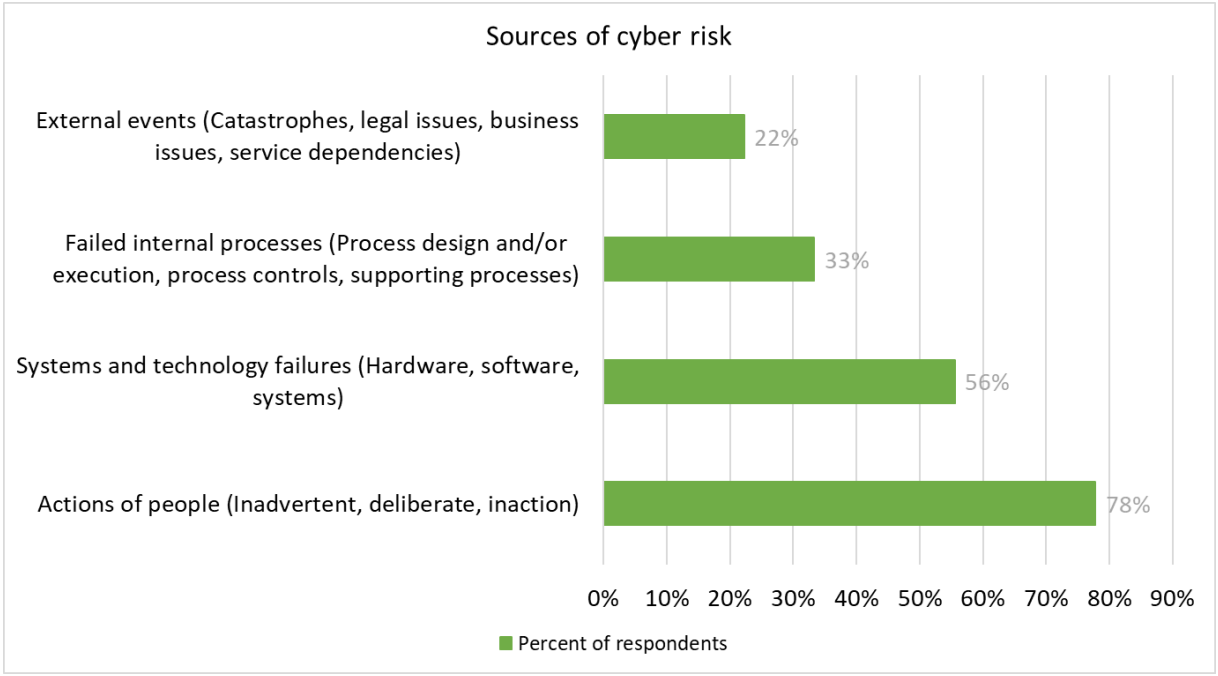


Figure 6.1 Banks' sources of Cyber Risk

The systems and technology failures like software, hardware and systems in general were considered the second major source of cyber risk for a bank with 78% of respondents contemplating it.

Regarding the main types of risk that banks are most exposed to, insurers unanimously consider data confidentiality breach as the major one. Malicious code attacks, cyber-extortion and cyber-fraud were also considered to be the most recurring incidents, as shown in figure 6.2.

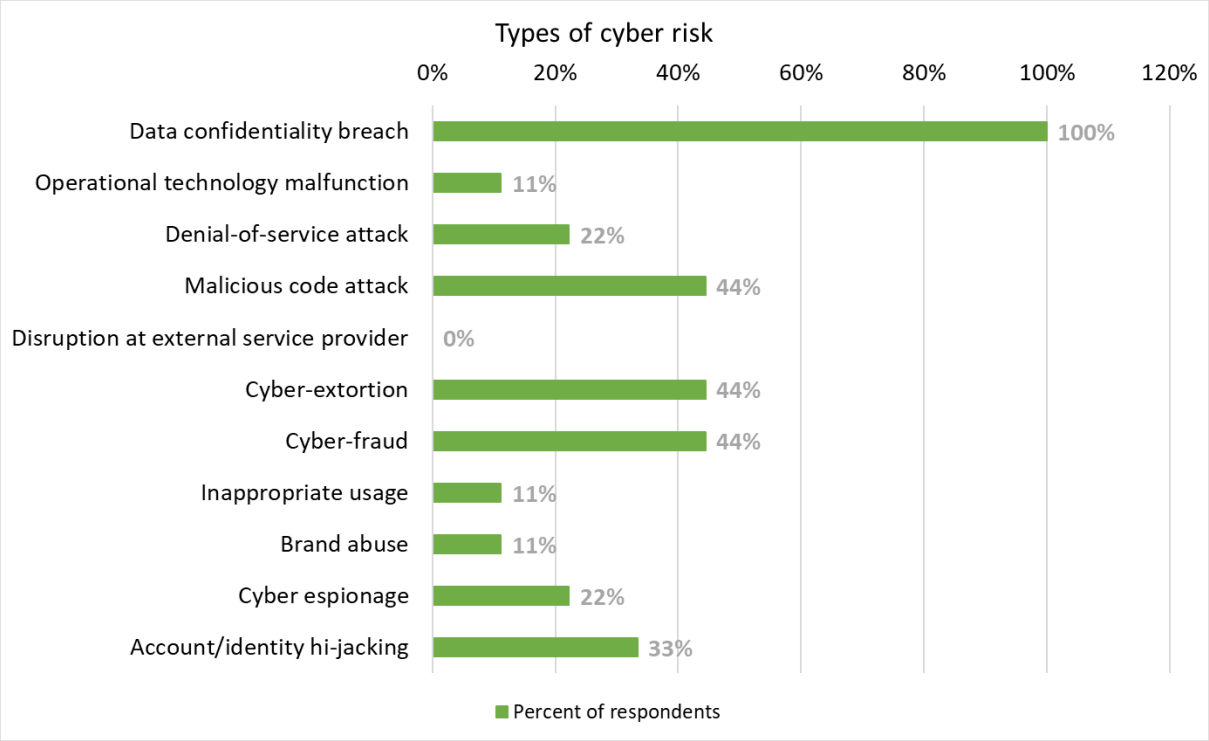


Figure 6.2 Banks' exposure to types of Cyber Risk

This perception is in line with what was found in the literature review. Banking institutions suffer from this type of attacks largely for financial reasons and for the purpose of extortion of money and compromising the data confidentiality. These are the main targets for criminals.

According to Banco de Portugal, banking institutions are exposed to financial, reputational, operational and legal risks. Figure 6.3 show that most participating insurers consider business interruption (operational risk), reputational damage (reputational risk) and financial loss from fraudulent electronic transfer of funds (financial risk) as the main impacts resulting from a cyber-attack.

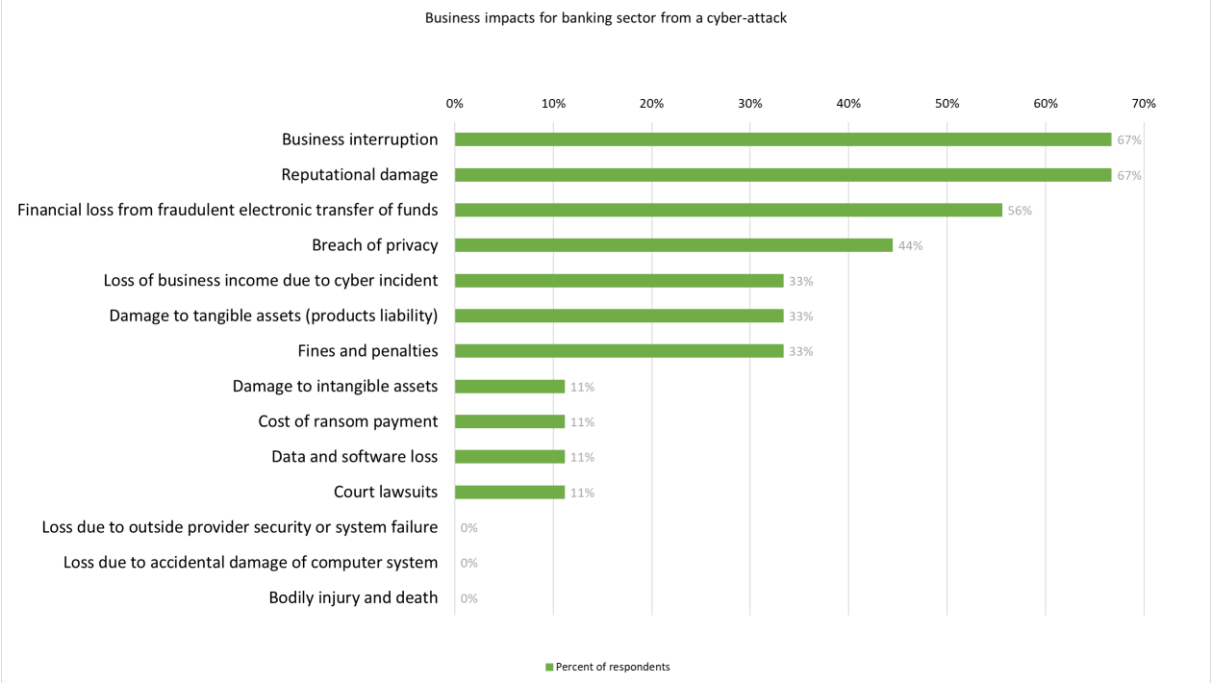


Figure 6.3 Impacts of cyber-attacks on banks

C. Cyber risk insurance

Regarding the offer of an insurance against cyber risk, only 2 of the participating insurers sell the product. Some of the reasons mentioned by the others for not offering this insurance were the lack of awareness to cyber risk, the lack of information to design and implement this kind of product and the very high costs associated with it. It was also pointed that there is still a small market in Portugal, which lacks scalability, and also a short demand. Besides that, the problems of which guarantees are covered and how the cyber-attack would be actually measured in case of a claim were also stated. In fact, some of those difficulties are the same as referred in chapter 4 (Underdeveloped causes) of the literature review.

The Portuguese market faces the same challenges international markets have faced and still face. This is mainly because we are still in the early steps of cyber risk insurance development in Portugal. Basically, insurers are beginning to realize the need for this product, but at the same time, there are still many factors to hold its development back.

The two insurers offering cyber risk sell it as a stand-alone product (a specific insurance for cyber risk) and one of them also sells a specific endorsement on existing policies (an add-on coverage to traditional lines of business). Both cover 1st party costs and one also cover 3rd party costs.

As with the study “Enhancing the Role of Insurance in Cyber Risk Management”, presented by the OECD in 2017, which graphically presents the loss categories commonly included in stand-alone policies, showed in subchapter 4.2.2 Coverages and exclusions of this work, figure 6.4 intends to apply the same research to the participating companies but focusing only in banking institutions. The results were the following:

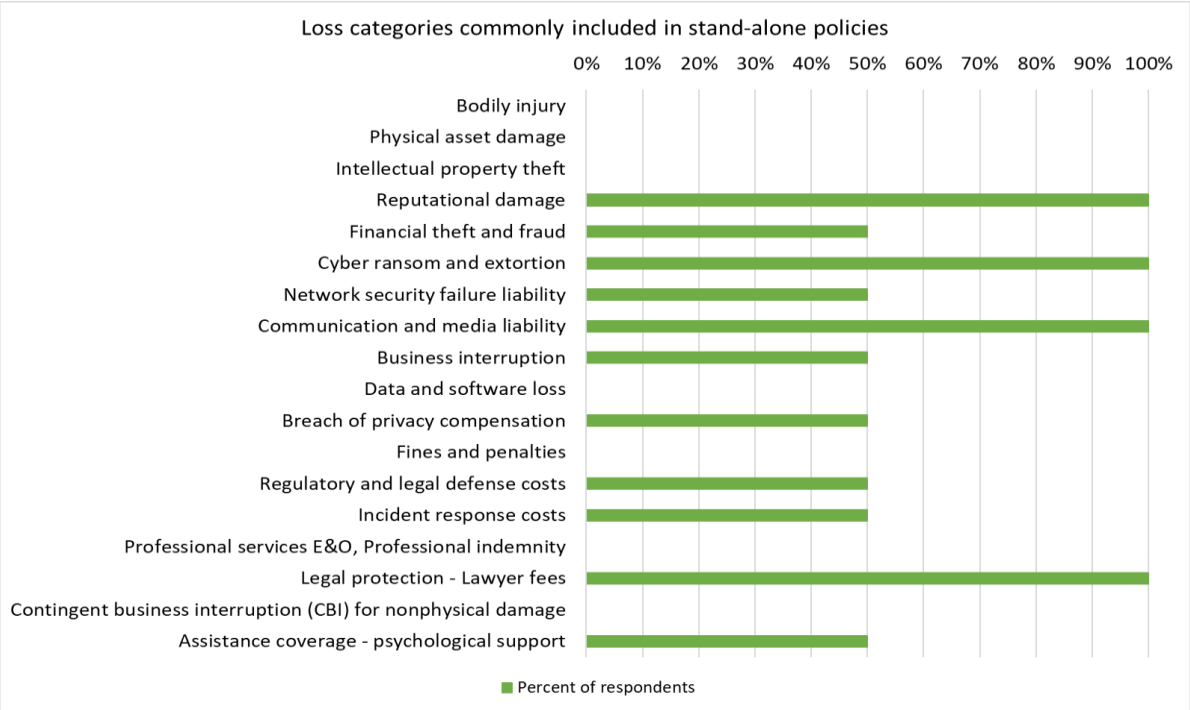


Figure 6.4 Loss categories commonly included in stand-alone policies

“Cyber ransom and extortion” and “Communication and media liability” were the loss categories stated by both participating insurers that correspond also to the most voted ones in the OECD study.

Reputational damage, as already stated above, is a loss that the financial sector is most exposed to and so it was referred by both insurers too, as the loss categories included in stand-alone policies offered to banks.

The last 4 categories (“professional services E&O and professional indemnity”; “legal protection - Lawyer fees”; “contingent business interruption (CBI) for nonphysical damage” and “assistance coverage - psychological support”) were added to the OECD list of loss categories. “Legal protection (lawyer fees)” was referred by both insurers as necessary to be included in stand-alone policies in the case of a bank costumer.

As mentioned in the literature review, the process of offering a product against cyber risk is often accompanied by a risk assessment. This serves not only so that insurers can analyze what type of risk their client is exposed to but also as to adjust their offer to each reality so as not to take too much unexpected risk.

When questioned about the implementation of cyber risk assessment in banks, only one of the insurers stated to do so. The practices adopted were self-assessment questionnaires applied to costumers, external support from specialized consultancies such as auditors and IT security consultants, who may perform e.g. penetration tests. The insurer affirm that its offer depends on the risk assessment made.

Additionally, there are some costumer´s criteria that insurers refer to assess, not in the context of a formal risk assessment. They are essentially policies and procedures of the institution, vendor

management systems (supply chain), data classification, log monitoring and network monitoring. Besides that, both insurers selling cyber insurance claimed to offer additional services with the product such as: risk management services, incident response services, cyber risk assessment, cash advance abroad, psychological counseling, 24/7 assistance or security check up. This shows the care taken by insurers to evaluate their client's cyber hygiene.

Furthermore, and in line with literature review, the insurers state that pricing is affected by technology prevention measures, procedures implemented and maturity of customers. It will ultimately persuade banks to improve their cybersecurity practices and to purchase a cyber insurance product.

Regarding the sale of a product against cyber risk, participating insurers were asked about the main obstacles or potential obstacles to the sale of this insurance. Figure 6.5 shows the answers:

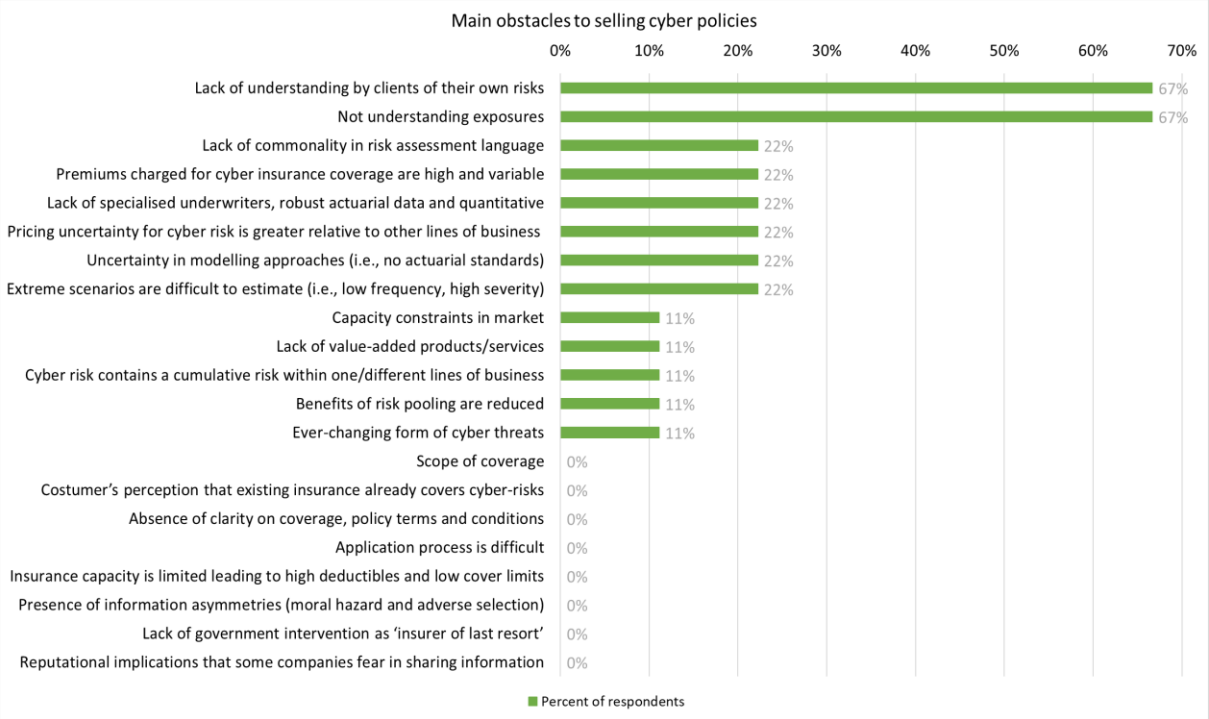


Figure 6.5 Main obstacles to selling cyber policies

The answers agree with the main reasons why most participating companies do not market the product, already discussed above. The lack of understanding by clients of their own risks and not understanding exposures were unanimously referred. In fact, the Portuguese market is still a few steps back when it comes to this subject.

However, although there is still a long way to go, there is actually already awareness to the fact that the development of an insurance dedicated to cyber risk brings numerous benefits to its customers. Among the options suggested in the questionnaire, 78% of insurers considered that this type of insurance promotes a greater organizational awareness of cyber risk and its potential impact on the business and endorses assessing the strength of cyber defenses (figure 6.6).

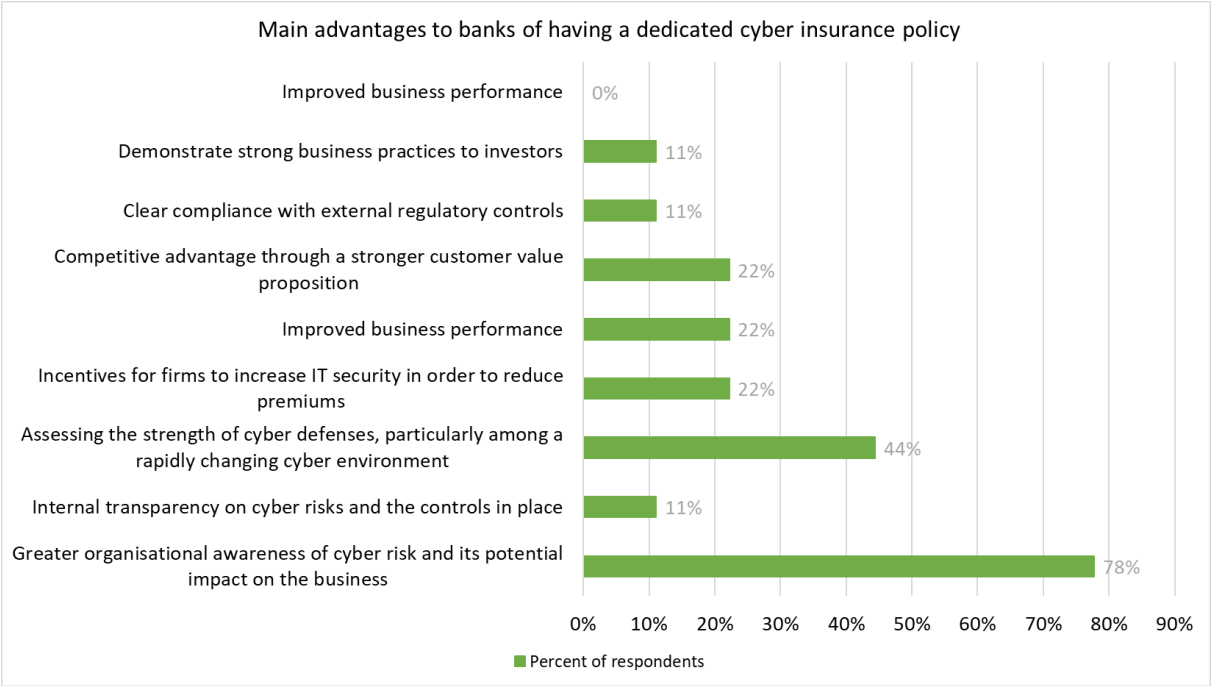


Figure 6.6 Main advantages to have a dedicated cyber insurance policy

Some authors considered that also government participation could boost the growth of the cyber insurance market. When taken in account the current state of cyber risk in Portugal, 56% of the companies believe so. Figure 6.7 shows how the participants considered the government should act.

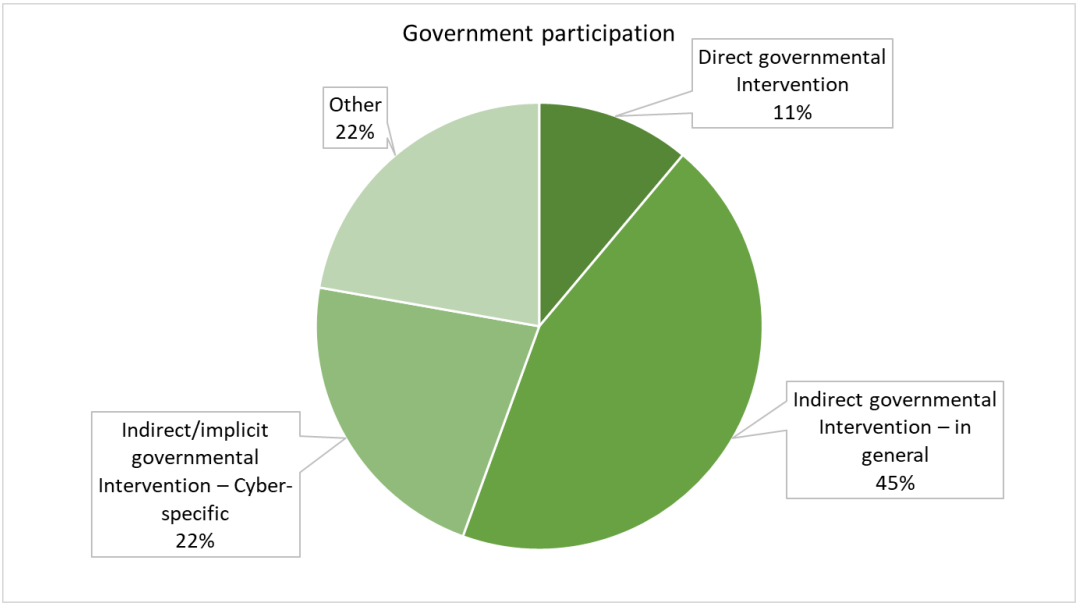


Figure 6.7 Ways of government participation in cyber risk insurance market

Indirect governmental intervention (in general) was indicated by 45% of the participants. This includes the implementation of cyber risk insurance as mandatory, carrying out incentives for self-insurance across subsidies through security spending or intensifying the penalties in case of

misbehavior. In addition, 22% of the participants referred that indirect/implicit governmental intervention (cyber specific) was the best way of intervention. This implied the creation of an anonymized data pool to exchange experience and information, the establishment or intensification of reporting obligations, the creation of new laws for data protection and the establishment of national standards for cyber risk in order to harmonize the principles for the market in general.

D. Perception of cyber risk's market evolution

This last section aims to capture the opinion of insurers regarding the evolution of the cyber insurance market. Most participating entities (56%) have been noticing an increase in the demand for cyber insurance products in the last 2 years.

It is the general opinion that the market will start or continue to grow in the coming years once the increase in awareness increases the demand. However, this growth is not expected to come easily since it requires much more clarification on the subject, both in terms of pricing, coverage, exclusions, exposure to risk, both on the side of the costumer and the seller.

As mentioned in the literature review, it is expected that the adoption of GDPR will accelerate the European market. The participating insurers share the same opinion, 78% of them consider that GDPR will ultimately increase awareness of cyber risk and stimulate demand for cyber insurance.

The last question asked was which controls should be applied to improve insurability of cyber risk. The development of regulation in order to standardize requirements, procedures and risk terminology and the development of platforms to exchange information about cyber incidents were the most voted options, as shown in figure 6.8.

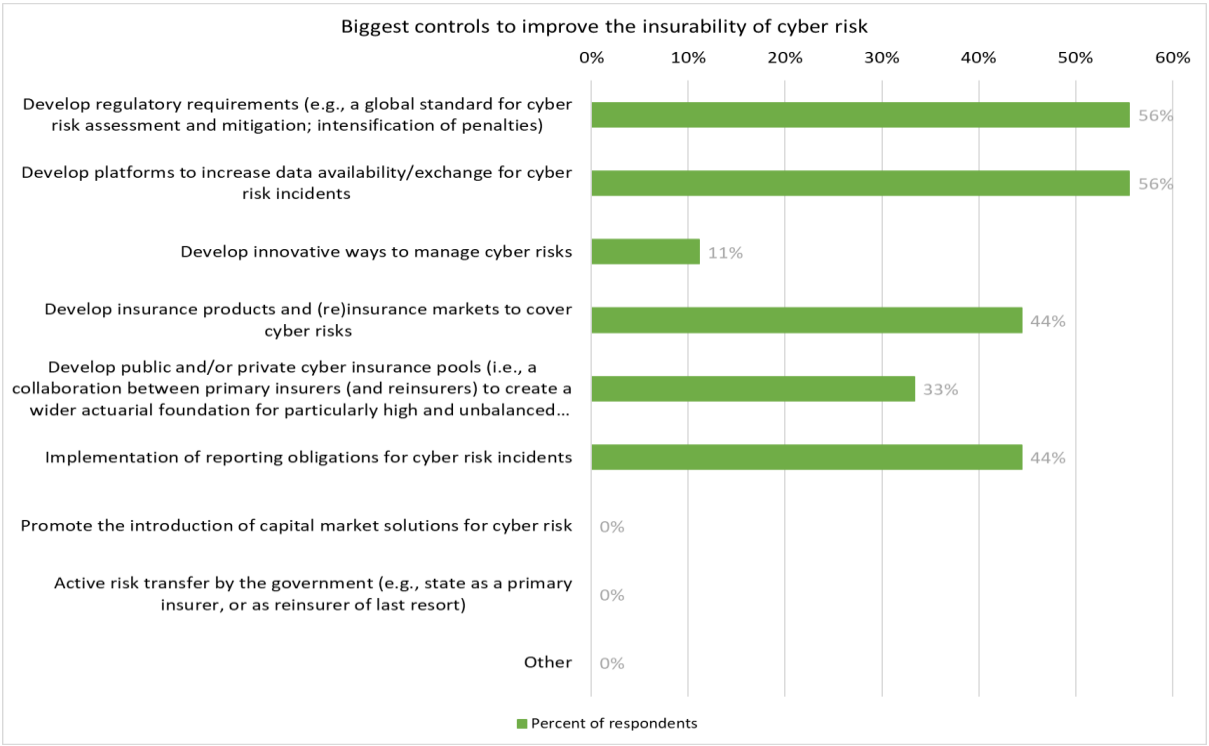


Figure 6.8 Biggest controls to improve the insurability of cyber risk

In fact, these could be measures that would help the market development through the spread of information and uniformization of the topic throughout the major intervenient (suppliers and customers). But it is still difficult to take the first steps in a topic that is still unknown and can have so many impacts to the costumer and to the insurer.

Supervisory Framework

Another aspect addressed in this work is the perspective of insurers in relation to the supervisory framework in the market for cyber risk. When asked whether the supervisory framework could in any way restrict market growth, most insurers (78%) responded that they did not.

In fact, many efforts have been made at European level, by EIOPA, on the issue of cyber risk and the new challenges it poses for the insurance industry. In Portugal, ASF and APS are the two entities that work together with market insurers, promoting the implementation of the Solvency II regime and the standardization of information throughout the market. Additionally, they raise awareness of this new risk.

In order to understand the perspective of the supervisory entity about the cyber risk insurance for banking sector, a questionnaire was applied to them. The questionnaire can be seen in annex 13.

As quoted by the ASF, they "*have been closely following the developments in the area since the recent past, not only from the point of view of cyber risks as a menace to the functioning of insurance undertakings (i.e. operational risks), but also from the point of view of insurers as cyber risk underwriters*".

Although they consider that the Portuguese cyber insurance market is in a very embryonic stage, they recognize its great growth potential. Besides that, they noticed that insurance companies in Portugal have included cyber risks in the top risks in the regular ASF's risk survey[7], which indicates an identification of the theme.

However, ASF also recognizes some challenges for an insurance company to secure this risk. "*The lack of information (largely associated to the fear of self-exposure in terms of cyber vulnerabilities) on cyber incidents makes it more difficult to quantify the effective exposure*" and "*the existence of silent or non-affirmative cyber covers, i.e. inadequately designed insurance policies which actually cover certain risks falling in the remits of cyber, but that have not been properly assessed/estimated*" were the ones pointed. The first one was also pointed by insurers meaning that the lack of information is generalized opinion.

When questioned about the preparedness of insurance companies operating in Portugal, under the ASF's supervision, to sell cyber insurance, they stated that it is a matter under assessment. In fact, "*the first undertakings offering cyber risk coverage in Portugal were entities operating globally, which had already developed this product in other countries, including outside the EU*". This is a lot due to all the difficulties that are being felt by the offer side already stated in the literature review.

[7] Report developed by ASF in August 2019, "Análise de Riscos do Setor Segurador e dos Fundos de Pensões". More details in https://www.asf.com.pt/NR/rdonlyres/BA3ED55C-B8B5-4571-B4D2-B1CAF507CCA0/0/An%C3%A1lisedeRiscosdoSetorSeguradoredosFundosdePens%C3%B5es2019.pdf

Another topic asked to the supervisor was about the contribution of GDPR for the increase awareness of cyber risk and stimulation of demand for cyber insurance. They recognize the importance of it once "*undertakings can now be exposed to majors' fines in case of a data breach, especially if it is a consequence of poor or inadequate cybersecurity*".

Finally, ASF was asked about possible controls to improve the insurability of cyber risk. This question was also requested from participating insurers and the answers were coincident. Like insurance companies, ASF also considers that the development of regulatory requirements, of platforms to increase data availability/exchange for cyber risk incidents and insurance products and (re)insurance markets to cover cyber risks are the best controls that could be adopted.

In ASF's perspective, "*it is important to develop a regulatory framework, according to which insurance undertakings adopt measures in order to prevent cyber incidents and reduce the probability of cyber-attacks. Hence, more than defining penalties for non-compliance, it is important to ensure that adequate measures are implemented in order ensure the confidentiality, integrity and availability of information*". In addition, "*from the point of view of risk taking, it is important to ensure that insurers are able to adequately assess the risks they are exposed to and avoid cyber risks concentration*".

Furthermore, in regard to the platforms to trade information on cyber incidents ASF considered that exchange of knowledge is very important and should be cultivated, e.g. by Governments, through their cybersecurity agencies, in order to have "complete, reliable and adequate data". "*The relevance of building such a data base goes beyond the insurance market, since it is relevant for all entities which have the intention to adopt adequate cybersecurity measures*".

About the development of insurance products and (re)insurance markets to cover cyber risks, the supervision believe that it is essential to have an appropriate delimitation of the coverages and for that "*cyber risk policies must define very clearly which risks are being covered and what are the exclusions*".

7. CONCLUSIONS

This work intends to study the offer of cyber insurance for banking sector operating in Portugal.

The literature review developed in this work aims to show how this new risk is being faced by insurers in the world and in Portugal, as well as the state of the art in relation to the development of insurance against this risk.

The empirical study carried out aims to assess how the insurance sector in Portugal (insurers and ASF) is reacting to this new risk, what specific actions to take in case a customer is a bank and how they perceive the evolution of the market in the country.

In fact, there is a great awareness in several countries around the world, including Portugal, that the actions of people, namely employees, are considered the greatest source of cyber risk for companies, both in the banking sector and in other sectors. These can be involuntary, through access to untrusted sites, emails that appear to be from secure sources or downloads, which jeopardize information security or volunteers, such as actions in bad faith.

Attacks such as data confidentiality breach, in which confidential information is used and disclosed, malicious code attacks, cyber extortion and cyber fraud are the types of risk that participating insurers consider to be the ones that banks are most exposed to having major impacts such as business interruption, reputational damage and financial loss.

So, participating insurers consider that their insurance offer to a bank should contain coverage against at least reputational damage, cyber ransom and extortion, communication and media liability. In fact, banking institutions operate based on the trust they generate in their customers, their reputation is fundamental to the success of their business. In addition, this sector is a major target for these types of threats since they are a source of money and sensitive information. That is why the above coverages are considered by the insurers to be the most important.

Although the insurance market in Portugal is aware of this new threat, there are still many aspects that make insurance against this risk not appealing, both for those who buy it and for those who sell it. The lack of understanding of risk exposure on the part of customers, who often consider themselves already protected against the risk.

The poorly standardized language in the underwriting process and the low clarification on coverages and exclusions are examples of that. Additionally, it is considered that the prices charged are too high and variable, making the purchase of the cyber insurance product unattractive. The lack of historical information makes it very difficult for insurers to develop robust actuarial models for estimating premiums and reserves, making the offer of this product not imperative.

Besides these aspects that hold the market back, insurers consider that insurance would be a good strategy to be adopted by banks since it would contribute alone to raise awareness of this risk and its potential impacts within institutions.

Finally, responding to the research questions proposed in this work, it is considered that the insurance companies operating in Portugal still do not have advanced knowledge about cyber risk. In addition, there is still no great offer of this product. However, participating insurers are aware of the possible exposures and impacts of a cyber-attack on a banking institution, which may indicate that when they develop cyber risk insurance, they will be aware of their client's needs.

Of the participating insurers, only two sell specific insurance for cyber risk. One of them performs a risk assessment to its client and considers it essential when offering the product. In addition, both insurers consider that technology prevention measures, procedures implemented, and maturity of customers influence the pricing of cyber risk products. This means that insurers are not willing to accept risk at any price and that they take into account the innumerous aspects of their client's awareness and security measures when offering insurance.

From the participating insurers and ASF's point of view, the development of the cyber risk insurance market is far from being at its peak, however it is expected to increase gradually over the next few years, although there are still many obstacles to overcome.

It is important, in their opinion, to create regulatory requirements, platforms for sharing information on cyber incidents and the development of insurance and reinsurance products against this risk in order to help the development of the market in the country.

It is the general opinion that this is a market that is taking its first steps in Portugal, but whose growth and development is inevitable.

8. LIMITATIONS AND RECOMMENDATIONS FOR FUTURE WORKS

Cyber risk, cybersecurity and cyber risk insurance are constantly evolving and also increasingly studied topics. However, as we see from the work done, there is still a lot of work to do and many gaps to be filled.

Initially the work was designed to cover the study of supply and demand for insurance against cyber risk. Questionnaires would be applied to insurers and also to banking institutions operating in Portugal, whether or not they purchased the insurance. The questionnaire to the banks was developed, but it was not applied due to the deadlines for delivering the thesis. The questions that make up the questionnaire can be seen in Annex 14. They essentially were intended to understand the demand side for insurance. I think it was one of the limitations of this work as it would enrich it.

So, the application of the bank's questionnaire is a future work recommendation since I think that it would be interesting to have the point of view from the institutions that buy besides from the ones that sell.

Another major limitation, or rather saying difficulty, was the approach to insurers. Since it is a rather sensitive and still unknown subject, some insurers preferred not to state their opinion on the topic, even though the questionnaires were anonymous.

Since this study focused on the perception and development of the cyber risk insurance market in Portugal, it would also be important to study the perspective of brokers and reinsurers on this subject.

To make the analysis even more complete, a survey could be made to the institutions that work alongside with insurance companies in assessing customer's risk in order to know their main challenges and what their opinion about market development and reception is.

9. BIBLIOGRAPHY

AIR. (2017). Insuring Cyber Risk. *What is holding cyber insurance back, and how can the industry push forward?*

Baezner, M., & Robin, P. (2017). *Stuxnet.*

Baitha, A. K., & Vinod, S. (2018). Session Hijacking and Prevention Technique .

Banco de Portugal. (2019). *Ciber-resiliência no setor bancário. A perspetiva do Banco de Portugal.*

Bernardo, C. (2018). Metade do PIB de Lisboa desapareceria com um terramoto. *Jornal Económico*.

Biener, C., Eling, M., & Wirfs, J. H. (August de 2014). Insurability of Cyber Risk.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: an empirical analysis.

Bloomberg. (2018). *Hackers Breach HealthCare.gov System, Get Data on 75,000*. Obtido de Bloomberg.

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*.

Cebula, & Young. (2010). A Taxonomy of Operational Cyber.

CEPS, & ECRI. (2018). *Cybersecurity in Finance.*

Comissão Europeia. (2003). Recomendacao da Comissao relativa à definição de micro, pequenas e médias empresas.

Deloitte. (2016). *Beneath the surface of a cyberattack.*

EBA. (2017). *Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2).*

EBA. (2018). *EBA draft Guidelines on ICT and security risk management.*

EBA. (2018). Risk Assessment Questionnaire.

EIOPA. (2018). *Understanding Cyber Insurance: a structured dialogue with insurance companies.*

Eling, M., & Wirfs, J. H. (2016). *Cyber Risk - Too Big to Insure?*

ENISA. (2012). Incentives and barriers of the cyber insurance market in Europe.

ENISA. (2016). *Cyber Insurance: recent advances, good practices and challenges.*

ESA. (2019). *Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector.*

Fluchter, K., & Wortmann, F. (2015). Internet of Things.

Forbes. (2018). *380,000 Passengers Affected By 'Malicious' British Airways Hack*. Obtido de Forbes.

Forbes. (2018). *How Facebook Was Hacked And Why It's A Disaster For Internet Security*. Obtido de Forbes.

Forbes. (2018). *Security Experts Weigh In On Massive Data Breach Of 150 Million MyFitnessPal Accounts*. Obtido de Forbes.

Forbes. (2018). *Steps To Take If The Marriott Data Breach Affected You*. Obtido de Forbes.

Forbes. (2018). *Ticket Site Hack Leaves 26 Million Users Exposed*. Obtido de Forbes.

Franke, U. (2017). The cyber insurance market in Sweden.

Garcia-Alfaro, J., & Navarro-Arribas, G. (2009). A Survey on Cross-Site Scripting Attacks.

Gupta, S. (2013). Types of Malware and its Analysis. *International Journal of Scientific & Engineering Research*.

IAIS. (2016). Issues Paper on Cyber Risk.

IMF, & Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.

IRM. (2014). *Cyber Risk: Resources for Practitioners.*

Kosub, T. (2015). *Components and Challenges of Integrated Cyber Risk Management.*

Lloyd's. (2017). Cyber Risk. *Cyber Secure*.

Marsh. (2018). *Governing Cyber Risk. A guide for company boards.* TheCityUK.

Marsh&McLENNAN. (2015). Helping you understand, quantify and manage Cyber Risk.

Marsh, & McLENNAN. (2018). *Cyber Risk Management. Response and Recovery.*

MDS. (2019). *Cyber Risk. Ameaça virtual versus ameaça real.*

Miková, T. (2013). *Cyber Attack on Ukrainian Power Grid.*

NATO. (2013). *Tallinn Manual on the International Law applicable to cyber warfare.*

OECD. (2016). OECD Project on Cyber Risk Insurance.

OECD. (2017). Enhancing the Role of Insurance in Cyber Risk Management.

OECD. (2017). Supporting an Effective Cyber Insurance Market. *OECD Report for the G7 Presidency*.

OECD. (2018). Enhancing the role of insurance in cyber risk management. *The cyber insurance market: Responding to a risk with few boundaries*.

Pierce, W. O. (2017). *Breaking Down the Equifax Data Breach.*

Reddy, M. L., & Bhargavi, V. (2018). Cyber security attacks in banking sector: Emerging security challenges and threats. *American International Journal of Research in Humanities, Arts and Social Sciences*.

Roy, A., & Sarkar, S. (2014). *Point of sale vulnerabilities: Solution approach.*

RSA. (2016). Cyber Risk Appetite: Defining and Understanding Risk in the Modern Enterprise.

Saini, D. K., Azad, I., Raut, N. B., & Hadimani, L. A. (2011). Utility Implementation for Cyber Risk Insurance Modeling. *World Congress on Engineering.*

Sidhu, J., Sakhuja, R., & Zhou, D. (2014). *Attacks on eBay.*

Woods, D., & Simpson, A. (2017). Policy measures and cyber insurance: a framework. *Journal of Cyber Policy*.

10. ANNEXES

Annex 1. Cyber incident potential cost and consequences

Cyber incident potential cost	Definition
Technical investigation	Direct expenses for analysis to determine what happened during a cyber incident and who was responsible. It involves digital forensics, malware and threat analysis to determine root cause to assist in the remediation and recovery of impacted systems, and to inform future cybersecurity improvements.
Customer breach notification	Expenses associated with informing and advising individuals whose data has been compromised (can include printing, mailing, and call center services), as typically mandated by state or federal law or industry regulation.
Post-breach customer protection	Costs associated with services to detect and protect against potential data breaches.
Regulatory compliance	Fines or fees charged as a result of non-compliance with federal or state cyber breach related laws and/or regulations.
Public relations	Costs associated with managing external communications or brand monitoring following an incident.
Attorney fees and litigation	Legal advisory fees and settlement costs externally imposed, and costs associated with legal actions the company may take to defend its interests.
Cybersecurity improvements	Expenses for technical improvements to the infrastructure, security controls, monitoring capabilities, or surrounding processes, specifically to recover business operations after an incident or to prevent a similar occurrence in the future.
Insurance premium increases	Additional costs an insured entity might incur to purchase or renew cyber risk insurance policies following a cyber incident.
Increased cost to raise debt	Organizations appear to be perceived as higher-risk borrowers during the months following a cyber incident facing higher interest rates for borrowed capital, either when raising debt, or when renegotiating existing debt.
Impact of operational disruption or destruction	Includes losses tied to manipulation or alteration of normal business operations and costs associated with rebuilding operational capabilities. This could include the need to repair equipment and facilities, build temporary infrastructure, divert resources from one part of the business to another, or increase current resources to support alternative business operations to replace the function of systems that have been temporarily shut down; it could also include losses associated with inability to deliver goods or services.

Lost value of customer relationships	During an initial triage period immediately following a breach, it can be hard to track and quantify how many customers are lost.
Value of lost contract revenue	Includes revenue and ultimate income loss, as well as lost future opportunity associated with contracts that are terminated as a result of a cyber incident.
Devaluation of trade name	Intangible cost referring to the loss in value of the names, marks, or symbols an organization uses to distinguish its products and services.
Loss of intellectual property (IP)	Intangible cost associated with loss of exclusive control over trade secrets, copyrights, investment plans, patents and other proprietary and confidential information, which can lead to loss of competitive advantage, loss of revenue, and lasting and potentially irreparable economic damage to the company.

Source: (Deloitte, 2016)

Annex 2. Cyber security incidents along the years in several sectors

Year	Target	Sector	The attack	Details/Consequences	Source
2007	TJX Companies	Retail sector	Data breach	The retailer announced that over 45 million of its customers' credit and debit cards had been compromised.	(Camillo, 2017)
2010	Nuclear Power Plant in Iran	Energy sector	Malicious code attack	Stuxnet is a malicious computer worm that target industrial control systems. It infected over 200 000 computers and caused 1 000 machines to physically degrade.	(Camillo, 2017) (Baezner & Robin, 2017)
2011	Sony PlayStation	Entertainment Sector	Data breach	Sony PlayStation attack exposed around 100 million user accounts brought the network down for nearly a month.	(Camillo, 2017)
2013	Target	Retail sector	Data breach	Theft of approximately 40 million payment card records (along with 70 million other information records such as addresses and phone numbers).	(OECD, 2016) (OECD, 2017)
2014	Steel mill in Germany	Industry sector	Data breach	Attackers had used stolen logins that gain access to the mill's control systems. The intrusion led to parts of the plant failing, meaning that the blast furnace could not be shut down as normal, resulting in significant damage.	(OECD, 2017) (Camillo, 2017)
2014	Sony Pictures	Entertainment sector	Data breach	A hacker revealed confidential data from the film studio Sony Pictures. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, and other information.	(OECD, 2016) (AIR, 2017)
2014	Ebay	Telecommunication sector	Data breach	Personal Information such as names, date of birth, email addresses, passwords, credentials used to access other accounts outside Ebay and other information was stolen due to theft of three corporate employee log-in credentials.	(Kosub, 2015) (Sidhu, Sakhuja, & Zhou, 2014)
2014	Burger King	Food sector	Hi-jacking	The company's Twitter account had been hacked where its name had been changed to McDonalds and its background replaced with an image of Fish McBites. In the hour it took for officials to regain control, hackers proceeded to send 53 tweets to the burger chain's more than 80 000 followers with jokes or offensive images.	(IRM, 2014)
2015	Anthem Health	Health Insurance	Data breach Phishing	Medical data breach resulted in 80 million records stolen. The hackers got access to sensitive information like names, birthdays, medical IDs, Social Security numbers and addresses.	(OECD, 2016)
2015	Power grid in Ukraine	Energy sector	Phishing	Attackers used spear phishing to plant malware which disabled computers that controlled the system. It was a large-scale power disruption affecting electricity distribution companies in Ukraine and their consumers.	(Miková, 2013) (OECD, 2017)

2016	Dyn	Business sector	Distributed denial of service attack	Distributed denial-of-service (DDoS) attack on domain name system provider Dyn shut down many of the world most popular websites, including Twitter, Spotify, GitHub, Netflix, Reddit, CNN and many others in the U.S. and Europe, for several hours.	(AIR, 2017) (Camillo, 2017)
2017	Equifax	Business sector	Data breach	Over the course of three months, hackers exploited a website application vulnerability to access the personal data of as many as 143 million Americans. The exposed data include names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers and credit card numbers.	(OECD, 2018) (Pierce, 2017)
2018	Marriott	Tourism sector	Data breach	The Marriott Hotel confirmed that up to 500 million hotel guests' information had been stolen in a data breach. The data breach was detected on September 10th but could date back to 2014.	(Forbes, 2018)
2018	British Airways	Tourism sector	Data breach	Approximately 380 000 travellers who purchased plane tickets on the British Airways website and mobile app were robbed of their personal data, including their full credit card information.	(Forbes, 2018)
2018	MyFitnessPal	Health sector	Data breach	Cyber criminals gained access to over 150 million usernames, emails and passwords.	(Forbes, 2018)
2018	Medicare and Medicaid	Health sector	Data breach	Hackers gained access to HealthCare.gov, the government's Affordable Care Act enrolment website, compromising the sensitive personal data of some 75 000 people.	(Bloomberg, 2018)
2018	Facebook	Telecommunication sector	Data breach	Facebook security breach exposes accounts of 50 million users.	(Forbes, 2018)

Annex 3. Cyber security incidents along the years in banking sector

Year	Target	The attack	Details/Consequences	Source
2010	Federal Reserve Bank of Cleveland	Data breach	Theft of 122 000 credit cards.	(IMF & Bouveret, 2018)
2011	Citigroup	Data breach	The customer information such as contact details and account numbers from over 200 000 bank's customers were compromised.	(CEPS & ECRI, 2018)
2012	Sveriges Riksbank	Distributed denial of service attack	DDoS attack left the website offline for 5 hours.	(IMF & Bouveret, 2018)
2012	Federal Reserve Bank of New York	Data breach	Theft of property software code worth 9.5 million dollars.	(IMF & Bouveret, 2018)
2013	Banco Central del Ecuador	Cyber-fraud	13.3 million dollars stolen from the account of the city of Riobamba at the central bank.	(IMF & Bouveret, 2018)
2014	JP Morgan	Data breach Phising	Names, emails and postal addresses, and phone numbers of account holders were obtained by hackers.	(OECD, 2016) (CEPS & ECRI, 2018)
2015	Central Bank of Azerbaijan	Data breach	Theft of thousands of bank customers' information.	(IMF & Bouveret, 2018)
2016	Tesco Bank	Data breach	About 9 000 customers had money stolen from their online banking accounts. All other customers were affected by a temporary suspension of Tesco's web banking system's operations.	(CEPS & ECRI, 2018)
2016	Bangladesh Bank	Cyber-fraud	The SWIFT credentials of the Bangladesh central bank were used to transfer 81 million dollars from its account at the Federal Reserve Bank of New York.	(IMF & Bouveret, 2018)
2016	Bank of Russia	Cyber-fraud	Cyber-attacks aimed at stealing 50 million dollars from correspondent bank accounts at the central bank, resulted in a loss of 22 million dollars.	(IMF & Bouveret, 2018)
2017	Many industries (including banks)	Cyber-extortion	The Wannacry ransomware attack exploited a known vulnerability in older Windows operating systems, encrypting files and demanding a ransom to be paid for the decryption key.	(OECD, 2018)
2017	Bank of Italy	Data Breach	Suspected hackers have accessed client data of Italy's biggest lender, UniCredit. The attacks were carried out through an external commercial partner, which UniCredit did not identify. Biographical and loan data from 400 000 client accounts was stolen.	(IMF & Bouveret, 2018)
2017	Many industries (including banks)	Malicious code attack	NotPetya is regarded as a malware responsible for destroying data on the target's hard disk. It is estimated that as a result of supply chain disruptions, consumer goods manufacturers, transport and logistics companies, pharmaceutical firms and utilities reportedly suffered, in aggregate, over 1 billion dollars in economic losses.	(IMF & Bouveret, 2018) (Marsh & McLENNAN, 2018)

Annex 4. Principles of Integrity, availability and confidentiality of data

Category	Definition	Examples
Integrity	Integrity issues relate to misuse of the systems, as is the case for fraud.	Cyber-attacks may use hacking techniques to modify, destroy or otherwise compromise the intregrity of data.
Availability	Availability issues are linked to business disruptions.	Denial of service attacks by botnets, for example, mau be used to prevent users from accessing data that would otherwise be available to them.
Confidentiality	Confidentiality issues arise when private information within a firm is disclosed to third parties as in the case of data breaches.	Cyber-attacks may target various types of confidential information, often for criminal gain.

Source: (IMF & Bouveret, 2018) and (IRM, 2014)

Annex 5. Sources classification of cyber risk

Categories of Cyber Risk by source classification	
Non-criminal Sources	
Act of nature	Power outage after a natural catastrophe; destruction of servers or computer facilities by flooding; fire
Technical defects	Hardware failure (for example data loss after a head crash of the hard-drive or a computer crash); bug in software
Human failure	Unintentionally disclosure of information on webpage; false report
Business/strategic changes	Changes in market or economic conditions; supplier changes or failures
Criminal Sources	
Physical attacks	Physical data theft (for example theft of confidential bank data by an employee)
Hacker attacks	Espionage of costumer data or sabotage of company processes (for example DoS attack; key logger or malware (for example virus, worms, spam-mails, Trojan horses)
Extortion	Threats by internet (for example Mexican drug cartel)

Source: (Eling & Wirfs, 2016)

Annex 6. Categories and subcategories of cyber risk by source classification

Categories/Subcategories of Cyber Risk	Definition	Elements	Non-ciminal/Criminal Sources
Actions of people			
Inadvertent	Unintentional actions taken without malicious or harmful intent. It can be internal unintentional or external unintentional depending if the human source of risk is within or without the organization (RSA, 2016)	Errors Omissions	Non-criminal - Human Failure
Deliberate	Actions taken intentionally and with intent to do harm. It can be internal malicious or external malicious depending if the source of risk is within or without the organization (RSA, 2016)	Fraud Sabotage Theft Vandalism Espionage Extortion	Criminal - Physical attacks; Hacker attacks; Extortion
Inaction	Lack of action or failure to act in a given situation	Lack of appropriate skills, knowledge, guidance and availability of employees to take action	Non-criminal - Human Failure
Systems and technology failures			
Hardware	Risks traceable to failures in physical equipment	Failure due to capacity, performance, maintenance, and obsolescence	Non-criminal - Technical defects
Software	Risks stemming from software assets of all types, including programs, applications, and operating systems	Compatibility, configuration management, change control, security settings, coding practices, and testing	Non-criminal - Technical defects
Systems	Failures of integrated systems to perform as expected	Design, specifications, integration, and complexity	Non-criminal - Technical defects

Failed internal processes			
Process design and/or execution	Failures of processes to achieve their desired outcomes due to poor process design or execution	Process flow, process documentation, roles and responsibilities, notifications and alerts, information flow, escalation of issues, service level agreements, and task hand-off	Non-criminal - Human Failure
Process controls	Inadequate controls on the operation of the process	Status monitoring, metrics, periodic review, and process ownership	Non-criminal - Human Failure
Supporting processes	Failure of organizational supporting processes to deliver the appropriate resources	Staffing, accounting, training and development, and procurement	Non-criminal - Human Failure
External events			
Catastrophes	Events, both natural and of human origin, over which the organization has no control and that can occur without notice	Weather event, fire, flood, earthquake, unrest	Non-criminal - Act of nature; Technical defects; Human Failure; Business/strategic changes Criminal - Physical attacks; Hacker attacks; Extortion
Legal issues	Risk arising from legal issues	Regulatory compliance, legislation, and litigation	Non-criminal - Human Failure
Business issues	Risks arising from changes in the business environment of the organization	Supplier failure, market conditions, and economic conditions	Non-criminal - Business/strategic changes
Service dependencies	Dependence on external parties	Utilities, emergency services, fuel, and transportation	Non-criminal - Act of nature; Technical defects; Human Failure; Business/strategic changes Criminal - Physical attacks; Hacker attacks; Extortion

Source: (Cebula & Young, 2010) and (Eling & Wirfs, 2016)

Annex 7. Examples of most common cyber incidents

Cyber Incident	Definition	Examples
Data confidentiality breach – third party or own data (Marsh & McLENNAN, 2018)	Data breaches take place when unauthorized individuals (employees or outsiders of organizations) accidentally or deliberately copy, transmit, view, stole or use valuable corporate data, such as credit card or bank details, personal health information (PHI), personally identifiable information (PII), trade secrets of corporations or intellectual property, to destinations outside of the organization's network borders (IRM, 2014) (IMF & Bouveret, 2018). It can be third-party or own data.	**Cyber espionage** (IAIS, 2016) - any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party (NATO, 2013); **Point-of-sale (POS) intrusions** (IAIS, 2016) - A POS application is used on the sales counter of large retailers across the world and has the ability to charge a debit or credit card over the web or mobile network in real-time (Roy & Sarkar, 2014); **Insider threats** - insiders or employees of banks can disclose, modify or access the bank information illegally. It can be also, unintentional errors by employees (Reddy & Bhargavi, 2018); **Crimeware** - any form of malware used for criminal purpose (IAIS, 2016).
Denial-of-service (DoS) attack or Distributed Denial-of-service (DDoS) (Marsh & McLENNAN, 2018)	A DoS is an attack in which a user or an organization is prevented from accessing a resource online. While as in DDoS attack, a specific system is targeted by a large group of compromised systems and make the services of the targeted system unavailable to its users (Reddy & Bhargavi, 2018).	The targeted system is flooded with incoming messages which causes it to shut down and thus the system is unavailable to its users. Although DoS attacks don't usually result in loss of information or security to a bank, it can cost the bank a great deal of time, money and customers and can also destroy programming and files in affected computer systems (Reddy & Bhargavi, 2018).
Malicious code attack (IAIS, 2016)	A malicious code attack is any infection or threat of infection by a malware. A malware is designed to secretly access a computer system without the owner's informed consent. The expression is a general term (short for malicious	**Virus** - Designed to copy itself and propagate from one computer file to another, usually by attaching itself to program files (Gupta, 2013); **Trojan horses** - A program that seems to be genuine and even useful, and thereby tricks the users to install/use it (Gupta, 2013); Worms - A worm will infect other computers, but do not propagate by infecting other

	software) used to mean a variety of forms of hostile, intrusive, or annoying software or program code (IAIS, 2016). It can be classified as crimeware (IAIS, 2016).	files (Gupta, 2013); **Ransomware** - Encryption of files on a computer, and leaving a message that a certain ransom must be paid for the decryption key to be disclosed (Gupta, 2013); **Adware** - software that enables displaying banner advertisements when the program is running (Gupta, 2013); **Spyware** - programs that collect information about a person or an organization without that entity's consent and awareness (Gupta, 2013); **Scareware** - comprises several classes of scam software with malicious payloads, or of limited or no benefit, that are sold to consumers via certain unethical marketing practices (Gupta, 2013); **Bot Networks** - Bots are programs that infect a system to provide remote command and control access via a variety of protocols, such as HTTP, instant messaging, and peer-to-peer protocols. Several of bots under common control are commonly referred to as a Botnet. Computers get associated with botnets when unaware users download malware which is sent as an e-mail attachment. Illicit activities can be carried out with bots by the controller that include relays for sending spam and phishing emails, updates for existing malware, DDoS, etc. (Reddy & Bhargavi, 2018); **Pharming** - It is also called farming or Domain Name System (DNS) poisoning. In this attack whenever a user tries to access a website, he/ she will be redirected to a fake site. Pharming can be done in two possible ways: one is by changing host's files on a victim's computer and other way is by exploiting vulnerability in DNS server software (Reddy & Bhargavi, 2018); **Phishing** - An attack in which an attempt is made to obtain user's sensitive information by an attacker pretending to be a reliable body in an electronic communication. It is typically carried out by email tricking or instant messaging in which users are asked to click on a link usually for securing their accounts. The users are then directed to fraudulent websites which look alike the original banking website so that the user is deceived and is asked to enter his personal information such as usernames, passwords, credit card details, etc. After that the fraudster has access to

		the customer's online bank account and to the funds contained in that account (Reddy & Bhargavi, 2018); **Rogueware** - Consists of any kind of fake software solution that attempts to steal money from users by attracting them into paying to remove nonexistent threats (Gupta, 2013); **Vishing** - It combines "voice" and —phishing. Vishing is an illegal practice where an attacker calls a user and pretends to be from a bank in which the user has an account. He usually asks to verify the user's account information (stating that user's account has been suspended, etc.) and once the user gives his credentials such as username, password, credit card number, etc., the attacker has easy access to the user's account and the money in it (Reddy & Bhargavi, 2018); **IP spoofing** - A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host (Gupta, 2013).
Cyber-extortion (IAIS, 2016)	It is usually accomplished through a form of crimeware known as ransomware in which hackers infiltrate computers encrypt the data and then demand a payment to decrypt it. Certain types of ransomware are very effective, and victims of such attacks cannot retrieve data without paying ransom unless they have made a backup copy of the data stored on media not subject to the ransomware attack (IAIS, 2016).	**DDoS** **Ransomware**
Cyber-fraud (Marsh & McLENNAN, 2018)	Illegitimate financial transfer is made as a result of a network intrusion or social engineering. Fraud is a kind of inappropriate behavior that is inherently malicious in nature, and aimed at personal enrichment by abusing company	**Phishing** **Vishing** **Ransomware** **Cyber-squatting** - A process in which a famous domain name is registered and then it is sold for a fortune. Cyber Squatters register domain names which are like popular

	systems, applications or information (Marsh & McLENNAN, 2018).	service providers' domains so as to attract their users and benefit from it (Reddy & Bhargavi, 2018); **SMS Tricking** - A user receives a SMS message which appears to be coming from a legitimate bank. In this SMS the originating mobile number (Sender ID) is replaced by alphanumeric text. Here a user may be fooled to give his/her online credentials and his/her money may be at risk of theft (Reddy & Bhargavi, 2018); **SMS OTP attacks** - SMS OTP is widely used as an identification and authentication method by many major financial institutions. It is a two-factor authentication method in which a password is created and sent by SMS whenever the users attempt authentication and the password is disposed of after use. Hackers can easily intercept the authentication codes sent by SMS via the mobile network (Reddy & Bhargavi, 2018).
Account/identity hi-jacking and weak authentication (IRM, 2014)	In hijackings, the attacker uses an exploit on a device to take over a session between this device and a host. It disconnects then the device from the communication. The server still believes that it is communicating to the original device and sends private information to the attacker.	**Browser hijacker** - The most generally accepted description for browser hijacking software is external code that changes your Internet Explorer settings (Gupta, 2013); **Click jacking** - is a malicious technique of tricking web users into revealing confidential information or taking control of their computer while clicking on apparently innocuous web pages (Gupta, 2013); **Session hijacking** - is an attack which is basically used to gain the unauthorized access between an authorized session connections. This is usually done to attack the social network website and banking websites (Baitha & Vinod, 2018).
Cross site scripting attacks	Attacks against web applications in which an attacker gets control of a user's browser in order to execute a malicious script (usually an HTML/JavaScript code) within the context of trust of web application's site. The injected script can either point the user transparently to a malicious server or allow the attacker to hijack	

	the user's session and to access to any sensitive browser resource associated to the web application (e.g., cookies, session IDs, etc.) (Garcia-Alfaro & Navarro-Arribas, 2009).	
SQL Injection Attack	A code injection technique that exploits security vulnerability in some computer software (Gupta, 2013).	
Systems and technology failures (Eling & Wirfs, 2016)	It covers what is related to hardware, software and system failures.	See more detail on subchapter 4.1.2, table 1.5 Categories and subcategories of cyber risk by source classification
External Events	It covers what is related to catastrophes, legal issues, business issues and service dependencies.	See more detail on subchapter 4.1.2, table 1.5 Categories and subcategories of cyber risk by source classification
Failed internal processes (Eling & Wirfs, 2016)	Operational IT risks due to poor systems integrity or other factors (IRM, 2014)	See more detail on subchapter 4.1.2, table 1.5 Categories and subcategories of cyber risk by source classification

Sources: (Eling & Wirfs, 2016), (IRM, 2014), (Gupta, 2013), (Baitha & Vinod, 2018), (Reddy & Bhargavi, 2018), (Marsh & McLENNAN, 2018), (Garcia-Alfaro & Navarro-Arribas, 2009) .

Annex 8. Risk transfer options

Risk taker	Risk transfer options
Risk owner (will first install risk control activities such as self-protection and self-insurance to reduce its risk exposure)	Private risk pool Industry-wide risk pool
Primary Insurer	Conventional insurance Insurance pool
Reinsurer	Proportional reinsurance Non-proportional reinsurance Reinsurance pool
Capital Markets	Insurance-linked securities
Governments/Taxpayer	State as primary insurer/ complete coverage Reinsurer of Last resort

Source: (Eling & Wirfs, 2016)

Annex 9. Most common first and third-party coverages

Liabilities source	Consequences
First party loss – direct loss incurred by the insured	
Network interruption	Loss of business income due to cyber incident Business interruption Damage to intangible assets Damage to tangible assets (products liability)
Network interruption Outside Security Provider (OSP)	Loss due to outside provider security or system failure
Cyber extortion	Cost of ransom payment Cyber specialist
Electronic data incident	Loss due to accidental damage of computer system
Cyber theft	Financial loss from fraudulent electronic transfer of funds Data restoration Extra expense System clean-up costs Administrative investigation and penalties
Third-party loss - liability coverage/losses to others	
Data protection and cyber liability	Liability claims Fines
Media liability	
Wrongful collection of information	
Media content infringement/defamatory content	
Violation of notification obligations	

Source: (EIOPA, 2018)

Annex 10. Means of governmental intervention

Governmental intervention	Govern Action	Definition
Direct governmental Intervention	Primary insurer	
	Reinsurer of Last Resort	Covers only some specific major risks
	Lender of Last Resort	Provide liquidity to (re-)insurers that are in need, after a catastrophic cyber event
Indirect governmental Intervention (in general)	Incentivize the purchase of insurance coverage through compulsory insurance, set incentives for self-protection/self-insurance through subsidies based on security spending or intensify the penalties in case of misbehaviour	
Indirect/implicit governmental Intervention (Cyber-specific)	Set up an anonymized data pool	Provides a common platform for data sharing
	Establish or intensify the reporting obligations	
	Improve standards for data protection through new laws for data protection	
	Establish national standards (minimal standards) for cyber risk.	

Source: (Eling & Wirfs, 2016)

Annex 11. Risk associated to cyber security incidents

Risk associated to cybersecurity incidents	Examples
Financial	Expropriation of funds and/or assets Losses of future revenue Security costs of systems and remediation; Court costs and/or resolution; Fees for non-compliance with contractual obligations and/or possible sanctions.
Reputational	Loss of confidence due to recurrence and/or exposure incident media coverage; Impact on business areas critical for trust in the sector; Image degradation due to non-compliance with regulatory requirements and/or possible sanctions; Data Disclosure sensitive (i.e. personal)
Operational	Disruption of critical functions and/or services essential for the public; System incidents, applications and networks and/or security breaches of information; Failures in integrating systems and networks outsourcing; Activation of business continuity and disaster recovery.
Legal	Failure to meet deadlines regulatory financial reports; Inability to respond to legal obligations to customers / consumers; Non-compliance with regulation AML / CFT; Loss of confidentiality and data integrity sensitive (i.e. personal). Possibility of occurrence of disputes.

Source: (Banco de Portugal, 2019)

Annex 12. Questionnaire to Insurance Companies

QUESTIONS TO INSURANCE COMPANY	SOURCE
A. General information of the company	
1) Origin of the company:	
B. Knowledge of cyber risk	
1) What is the level of understanding about cyber risk?	(ENISA, 2016)
2) In your perspective, what sources of cyber risk are banks most exposed to?	(Cebula and Young, 2010)
3) In your perspective, what types of cyber risk a bank is most exposed to?	(OECD, 2018) (Marsh & McLENNAN, 2018)
4) What will be the business impacts for the banking sector from suffering a cyber-attack?	(EIOPA, 2018)
C. Cyber risk insurance	
1) Does your company sell insurance against cyber risk?	
2) What are the main reasons for not to commercialize an insurance product against cyber risk?	
3) What type(s) of cyber insurance coverage does the company offer?	(EIOPA, 2018) (OECD, 2017)
4) Does your company offer coverage of both 1st party costs and 3rd party liabilities?	(ENISA, 2016)
5) What loss categories does your company offer coverage?	(OECD, 2017) (Marsh & McLENNAN, 2018)?
6) Are there any exclusions regarding some types of cyber risks?	(Franke, 2017) (Marsh & McLENNAN, 2018) (EIOPA, 2018) (Biener, Eling, & Wirfs, 2015)
7) Does your company provide cyber coverage for subsidiaries and corporate entities in different jurisdictions?	(Franke, 2017)
8) Does your company assess the banks' exposure to cyber risk?	(Franke, 2017)
9) What are the requisites that a costumer must have in order to be eligible to get a cyber risk offer from your company?	(Franke, 2017)
10) How does your company assess bank's exposure to cyber risk?	(ENISA, 2012) (ENISA, 2016) (AIR, 2017)
11) Which costumer´s criteria do your company assess?	(ENISA, 2016) (Marsh, 2018) (Camillo, 2017) (EIOPA, 2018)
12) Does your cyber risk protection offer depends on the assessment that you do on your client?	(Franke, 2017)
13) Does your cyber insurance offering face certain challenges regarding the risk assessment of potential clients?	(ENISA, 2016)

14) Does your cyber insurance offering require or recommend a particular standard or good practice for assessing the risk of a potential client?	(ENISA, 2016)
15) Do you offer any additional services with the cyber insurance?	(EIOPA, 2018)
16) Is pricing affected by the technology prevention measures and procedures implemented by customers and maturity of customers?	(Franke, 2017)
17) In your perspective, what are the main obstacles to selling cyber policies?	(ENISA, 2016) (Eling & Wirfs, 2016)
18) In your perspective, what are the main advantages to the banks to have a dedicated cyber insurance policy?	(EIOPA, 2018)
19) In your perspective, do you think government participation would help the development of the insurance market for cyber risk?	(EIOPA, 2018)
20) In which way?	
D. Perceived market evolution for cyber risk	
1) Has the company been noticing an increase in the demand for cyber insurance products in the last 2 years?	(EIOPA, 2018)
2) How does the company perceive the future perspectives for the cyber insurance market?	(EIOPA, 2018)
3) Do you expect that GDPR will ultimately increase awareness of cyber risk and stimulate demand for cyber insurance?	(EIOPA, 2018)
4) In your opinion, are there any obstacles in the current supervisory framework that could ultimately restrain the growth of the cyber insurance market?	(ESA, 2019)
5) In your opinion, what are the biggest controls to improve the insurability of cyber risk?	(Eling & Wirfs, 2016)

Annex 13. Questionnaire to ASF

QUESTIONS TO INSURANCE COMPANY
1. How does the Supervision Authority perceive the evolution of cyber insurance market in Portugal?
2. What are the main challenges for an insurance company to secure this cyber risk?
3. Do you think that banking institutions operating in Portugal are properly prepared against cyber risk?
4. Do you expect that GDPR will ultimately increase awareness of cyber risk and stimulate demand for cyber insurance? Why?
5. In ASF point of view, what are the biggest controls to improve the insurability of cyber risk? (choose the best three options) a. Develop regulatory requirements (e.g., a global standard for cyber risk assessment and mitigation; intensification of penalties) b. Develop platforms to increase data availability/exchange for cyber risk incidents c. Develop innovative ways to manage cyber risks d. Develop insurance products and (re)insurance markets to cover cyber risks e. Develop public and/or private cyber insurance pools (i.e., a collaboration between primary insurers (and reinsurers) to create a wider actuarial foundation for particularly high and unbalanced risks) f. Implementation of reporting obligations for cyber risk incidents g. Promote the introduction of capital market solutions for cyber risk h. Active risk transfer by the government (e.g., state as a primary insurer, or as reinsurer of last resort) i. Other

Annex 14. Questionnaire to Banks

QUESTIONS TO BANKS	SOURCE
A. General information of the company	
1) Origin of the company:	
2) Number of employees and annual turnover:	(Comissão Europeia, 2003)
B. Knowledge of cyber risk	
1) What is the level of understanding about cyber risk?	(ENISA, 2016)
2) What are the company biggest exposures?	(IRM, 2014)
3) What are the main sources of cyber risk that the bank is exposed to?	(Cebula and Young, 2010)
4) What are the main types of cyber risk that the bank is most exposed to?	(OECD, 2018) (Marsh & McLENNAN, 2018)
5) What will be the business impacts for the bank from suffering a cyber-attack?	(EIOPA, 2018)
C. Cyber Attack History in the Enterprise	
1) Has the bank ever suffered a cyber-attack?	
1.1) What were the sources of that attack?	(Cebula and Young, 2010)
1.2) What were the types of cyber risk of that attack?	(OECD, 2018) (Marsh & McLENNAN, 2018)
2) Have your partners or outsourcing companies already suffered any cyber-attacks that have affected the bank?	
D. Cyber Insurance protection	
1) How do you manage cyber risk?	
1.1) Mitigation techniques	(EBA, 2018)
1.2) Transferring options	(Eling & Wirfs, 2016)
1.3) Other. Which?	
E. Cyber risk Insurance	
1) Does your company have cyber risk insurance?	
2) What type(s) of cyber insurance coverage does the bank purchase?	(OECD, 2017) (EIOPA, 2018)
3) Does the company already seek for insurance coverage for cyber risk?	
4) What are the reasons why the company doesn't have insurance against cyber risk?	(EIOPA, 2018)
If you select option d) (perception that the company is already protected against cyber-risks), indicate these forms of protection:	(Eling & Wirfs, 2016)
5) Does your cyber insurance covers both 1st party costs and 3rd party liabilities?	(ENISA, 2016)
6) What loss categories are included in your policy?	(OECD, 2017) (Marsh & McLENNAN, 2018)
7) When you made your insurance, contract was there any kind of cyber risk that the company considered important, and which the insurer did not cover?	
8) Did the insurer do any risk assessment to the company in the underwriting process?	

If the answer was yes, has this process assessed the following options?	(ENISA, 2016) (Camillo, 2017) (Marsh, 2018) (EIOPA, 2018)
9) Did the insurer apply some reduction to the premium due to the risk assessment findings?	
10) Does the company purchase any consulting, cyber risk assessment or incident response services from the insurance company?	(ENISA, 2016)
11) What are the main challenges found when purchasing a cyber risk insurance product?	(ENISA, 2012) (IRM, 2014) (Eling & Wirfs, 2016) (ENISA, 2016) (EIOPA, 2018) (OECD, 2018)
12) What are the main advantages to the company to have a dedicated cyber insurance policy?	(EIOPA, 2018)
13) How satisfied is the company with its cyber insurance product?	
14) Does the company follow any security management standards like ISO27001?	(ENISA, 2016)
F. Perceived market evolution for cyber risk	
1) How does the company perceive the future perspectives for the cyber insurance market?	(EIOPA, 2018)
2) Do you expect that GDPR will ultimately increase awareness of cyber risk and stimulate demand for cyber insurance?	(EIOPA, 2018)
3) In your opinion, what are the biggest controls to improve the insurability of cyber risk?	(Eling & Wirfs, 2016)

Annex 15. Glossary

Term	Definition
Cloud	It is well known as cloud computing and it is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software.
Crimeware	It is any computer program designed for the express purpose of conducting malicious and illegal activities online. Although adware, spyware and malware can all be used to conduct illegal activity, crimeware refers to programs that are meant to automate the theft of information, allowing the thief to gain access to a person's financial accounts online.
Cybersecurity	The term refers to strategies, policies, and standards encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience, and recovery activities, and policies regarding the security of an insurer's operations
Cyberspace	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers
Cyber-attack	Includes a wide range of technical and social methods to pursue an ultimate goal – the propagation, extraction, denial or manipulation of information. Attempts to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network.
Cybercrime	Includes a wide swath of activities that affect both the individual citizen directly (e.g. identity theft) and corporations (e.g. the theft of intellectual property)
Cyber extortion	Usually accomplished through a form of crimeware known as ransomware in which hackers infiltrate computers belonging to a business or an individual, encrypt the data thereon, and then demand a payment to decrypt it.
Cyber hygiene	It is defined "as a means to appropriately protect and maintain IT systems and devices and implement cybersecurity best practices". To be effective these measures of prevention, detection and action need to be attainable, accreditable and affordable
Cyber incident	Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.
Cyber insurance	It is one of the risk transfer mechanisms to address the financial costs that arise from cyber-attacks
Cyber-resilience	The ability to anticipate, withstand, contain and rapidly recover from a cyber-attack

Cyber risk	Cyber risk is commonly defined as exposure to harm or loss resulting from breaches of or attacks on information systems. However, this definition must be broadened. A better, more encompassing definition is "the potential of loss or harm related to technical infrastructure or the use of technology within an organization."
Cyber threat	A circumstance or event with the potential to intentionally or unintentionally exploit one or more system vulnerabilities resulting in a loss of confidentiality, integrity, or availability
Data Breach	It is an incident that involves the unauthorized or illegal viewing, access or retrieval of data by an individual, application or service. It is a type of security breach specifically designed to steal and/or publish data to an unsecured or illegal location. A data breach is also known as a data spill or data leak.
Hacker	A hacker is an individual who uses computer, networking or other skills to overcome a technical problem. The term hacker may refer to anyone with technical skills, but it often refers to a person who uses his or her abilities to gain unauthorized access to systems or networks in order to commit crimes
Emerging risk	Risks that are known to some degree but are not likely to materialize or have an impact for several years. Another characteristic of an emerging risk is that it can be very difficult to quantify as it can have far reaching impacts on industry and society overall.
Exclusion	Those risks excluded from an insurance policy
Gramm-Leach-Bliley Act	It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information.
HIPAA	Health Insurance Portability and Accountability Act is an act created by The United States Government in an effort to protect individuals covered by health insurance and to set standards for the storage and privacy of personal medical data.
HITECH	The HITECH Act was created to motivate the implementation of electronic health records (EHR) and supporting technology in the United States. The Act expanded the scope of privacy and security protections available under HIPAA compliance by increasing the potential legal liability for non-compliance and it providing for more stringent enforcement.
Information Technology	Information technology (IT) refers to the development, maintenance, and use of computer software, systems, and networks. It includes their use for the processing and distribution of data
Insurance Policy	It is the document defining what risks or perils are insured along with exclusions
Insurer	The party providing an insurance product
Insured	The party having taken out or likely to acquire or renew an insurance product
ISO 27000	It is a series of best practices to help organizations improve their information security.

family	
Liability	The state of being legally obliged and responsible under the terms of a policy
Network	It is a group of two or more devices that can communicate. In practice, a network is comprised of a number of different computer systems connected by physical and/or wireless connections.
PCI-DSS	It is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.
Premium	The fee paid by the insured to the insurer for assuming the risk
Self-insurance	Reduction in the size of a loss (the insured covering the costs of a loss itself
Self-protection	Measures taken by the insured to reduce the probability of a loss
Server	It Is a computer, a device or a program that is dedicated to managing network resources.
Systemic risk	It is the possibility that an event at the company level could trigger severe instability or collapse an entire industry or economy.
Ransom	It is a sum of money demanded in exchange for someone or something that has been taken.
Ransomware	Ransomware is a type of malware program that infects, locks or takes control of a system and demands ransom to undo it. Ransomware attacks and infects a computer with the intention of extorting money from its owner.
Risk aggregation	Defined as the process of defining, gathering and processing risk data.
SOX	Sarbanes-Oxley Act set standards related to data protection, applying to US public companies and accounting firms.