



LUISS GUIDO CARLI University

Department of Economics and Finance

Bachelor Degree in Economics and Business

CHAIR OF MONEY AND BANKING

The Impact of cyber-attacks in the financial sector

An analysis of the legal environment and the economic consequences of cyber crime

SUPERVISOR:

Prof. Paolo Paesani

CANDIDATE:

Giorgio Giannuzzi 235961

Academic Year 2020-2021

TABLE OF CONTENTS

<i>ACKNOWLEDGMENTS</i>	3
<i>INTRODUCTION TO THE THESIS</i>	4
<i>1.CHAPTER ONE-The cyber-environment and its risks</i>	6
<i>1.1 The Cyber-space</i>	6
<i>1.2 Cyber-crime</i>	8
<i>1.3 Cyber-attacks in the financial sector</i>	12
<i>2.CHAPTER TWO-The economic consequences of cyber-attacks</i>	21
<i>2.1 The economic impact of cyber-attacks in the financial sector</i>	21
<i>2.2 A practical case study: Cosmos SWIFT/ATM cyber-attack</i>	38
<i>3.CHAPTER THREE-Governments and Central Banks oversight and regulation</i>	40
<i>3.1 Cybersecurity Law and International cooperation</i>	40
<i>3.2 The U.S Cybersecurity legal framework</i>	47
<i>3.3 The European legal Framework and the European Central Bank</i>	53
<i>3.4 Italy: The national legal framework and the National Cybersecurity Perimeter</i>	63
<i>CONCLUSIONS AND FINAL REMARKS</i>	66
<i>BIBLIOGRAPHY AND SITOGRAPHY</i>	68

ACKNOWLEDGMENTS

First of all, I would like to thank my supervisor, Professor Paolo Paesani, for allowing me to discuss a topic of interest and helping me through the writing of this final dissertation thesis.

I would also like to thank my family for backing me up me both through good and bad times, for constantly transmitting me the right values and for always giving me the right advice. Your support has been fundamental for the success of my university career.

Then I desire to thanks all those friends who helped me during these three years and before. Even though I didn't want to make a list, each of you deserves to be thanked. Thank you Nicolò for supporting my university choice and for helping me whenever I needed it. Thanks, Ludovico, Filippo, and Matteo for being there for me since elementary school. Thank you Edoardo and Filippo for always having the right advice and never letting me down. Thanks, Goffredo, for supporting me and giving me always the most useful insights. And also thank you, Giordano, for helping me whenever I needed it. You all have been there for me through the ups and downs. You are more than just friends to me; you are my life companions.

Then I would like to thanks all those people that shared this path with me. Thank you, Gabriele, we shared everything, and thanks to you this road hasn't been uphill. Thanks, Filippo, you always supported me. And I would also like to thank Edoardo, Ruben, Carlo, Fabio, Marco, Dario, Daniele, and Tommaso, for backing me up and for making everything easier.

It hasn't been easy, but with the support of all those people and many more, I managed to overcome the difficulties I faced. This is not an arrival point, but only the starting point for something bigger.

INTRODUCTION

In today's world, the dynamics that previously were carried out physically and personally are increasingly shifted on the web, precisely in cyberspace. Cyberspace is a world unto itself, that has connections with all the dynamics performed in the real world: It connects people, public and private institutions, and all those actors that need to be connected to carry out their activities. In particular financial institutions heavily rely on the use of cyberspace, since it allowed to facilitate a lot of activities that in the past took more time and more money to be carried out. The possibility to increase the speed of transactions, to allow communications with countries which are distant, and to safeguard and facilitate the use of money, has led to the development of different technologies, such as credit and debit card, home and internet banking and so on. Financial intermediaries of all kinds rely on those technologies for the functioning and success of day-by-day operations.

The increasing amount of connections lead to an increased amount of data to store, carry and protect. The evolution of technologies aims at ensuring an augmented space for data storing and increased soundness of cyberspace. In this contest, not all the actors moving in cyberspace aim at exploiting it for a good purpose. Since the born of the internet, cybercriminals have started to search for vulnerabilities to exploit for their profit, and their scope has increased with the use of information technologies in each sector of the economy. Their main targets, alongside money, are data. Moreover, the covid pandemic led to an increment in the diffusion of smart-working activities, further increasing the activities carried out on the web and thus the need for safer cybersecurity infrastructures.

This thesis aims at analyzing the dynamics occurring in cyberspace that can directly affect the economic environment and financial stability. The analysis starts with an introduction of the generic cyber environment, the area in which all the activities of interest are carried out. Then it introduces some important aspects concerning cyber-crime, as its definition and the analysis of data concerning ICT security, such as the growth of cybercrime in the latest years both in Italy and around the world. The first chapter ends with research concerning the criminals active in the sector of interest, the most common attacks used, and some of the preferred targets by those criminals. It also analyzes the cost, both direct and indirect arising from cyber incidents, that are increasing with the sophistication of the attacks suffered.

The second chapter studies more in-depth the economic impact of cyber-attacks in the financial sector, introducing the concerns of Christine Lagarde about the possible financial implications of a systemic cyber-attack, the models developed by the European systemic risk Board to quantify the costs and consequences of different cyber incidents, and the characteristics that can lead to a systematic event that could threaten the soundness and stability of the financial sector as a whole. After presenting data on the effect of cybercrime on different components of the financial sector, such as the stock market, it analyzes the possible economic consequences by analyzing hypothetical case studies of specific kinds of cyber-attacks on financial institutions. The economic analysis ends with a real case study, concerning a sophisticated attack that affected Cosmos Bank, a financial institution of great importance active in India and other countries, that spread rapidly across 28 countries.

The last chapter analyzes the legal framework employed to face the increasing threats posed by cybercriminals. It first presents the initiatives undertaken by different international bodies of great importance, that aim at guaranteeing an adequate and coordinated response to the increasing threat posed by cybercriminals. Then it analyzes the fragmented legal framework of the U.S, with some federal laws and regulations and some state-specific acts, regarding the two states in which cyberspace is more used, the state of California and the state of New York. It follows an analysis of the main pieces of legislation active in Europe, where the legislation is less fragmented and wants to guarantee a common response to offer a higher level of cybersecurity. The last paragraph introduces briefly the Italian legal framework, which is based on the directives enacted by the European Union, and the creation of the cybersecurity perimeter.

The key findings of this analysis are linked to the greatest attention needed by both public and private actors in facing the problems that are linked to cybersecurity. The need for an increased level of supervision and cooperation among all the actors is fundamental to guarantee the economic stability needed by all the participants in the market. Without an adequate level of security, there is not enough confidence in the financial sector, and without confidence, the risks of systemic crises increase exponentially.

CHAPTER ONE

The cyber environment and its risks

1.1 THE CYBER-SPACE

The pervasiveness progressively assumed by the digital dimension concerning the dynamics characterizing the technical, industrial, social, and security process is so relevant that it can be defined as a real digital revolution. In particular, it is useful to define **cyberspace** as the overall IT interconnected infrastructures, including hardware, software, data, and users as well as the logical relationships mutually established between them. It comprehends the Internet, communications networks, and all those systems on which are based the IT process of data analysis and every device with an internet connection. Therefore, cyberspace can be considered a productive and social ecosystem deeper than the technological one from which it derives. Within cyberspace, there exists a strong link between the technological element and human interaction. As reported by Ottis & Lorents, the NATO Cooperative Cyber Defence Centre of Excellence¹ defines cyberspace as "*a time-dependent set of interconnected information systems and the human users that interact with these systems*".

The evolutionary process of cyberspace, boosted by the advent of the internet, has led to a progressive transition in the digital dimension of those activities previously developed in the dynamics of the real world, thanks to the breaking down of spatial and temporal boundaries. An enormous amount of data coming from the financial and social world and from organizational processes, stratified in the digital ecosystem over time in open data format. This evolution has built a common knowledge base enabling a multitude of new processes, services, and systems.

¹ Ottis, R., & Lorents P., (2010), Cyberspace: Definition and Implications. In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited. (pp 267-270)

That is true regarding all those critical infrastructures of interest in this analysis, as the financial and economic infrastructure, whose dependence on IT is increasingly pervasive, with all the following repercussions in terms of security.

Therefore, we can say that cyberspace is an enabling factor indispensable for all those activities and processes which were previously carried out with limited support of the ICT. On the other hand, the digital ecosystem has created the foundations for new forms of activities and new actors. In this regard, we can think about the central role assumed in modern society by the internet and mobile banking, smart and debit cards, cryptocurrencies, trading platforms, and other important tools. To sum up we can define cyberspace as the virtualization of human reality resulting from the common translation of every process from a physical to a virtual layer and space.

For these reasons, the Banking sector is directly affected by these changes and works to meet up with the new needs of its clients and the financial sector as a whole, keeping also in mind to maintain the soundness and trust which are needed in such an important industry. In this contest, it is important to underline that the interconnection between central banks and the financial sector with all its players is a fundamental element that needs to be taken into account when assessing the new scenarios of cyber risk. This interdependence between banks given by the digital connections could potentially lead to the spread of a cyber-attack through the whole financial system threatening its stability. Moreover, Financial institutions are a primary target of cyber-attacks.

1.2 THE CYBER-CRIME

The fast expansion in Cyberspace usage and the increasingly strong dependence of the society on its infrastructures led to an exponential growth in its threats, vulnerabilities, and risks. For our analysis, we are going to analyze the biggest phenomenon affecting the financial sector and its players, **cybercrime**.

As defined by the European Commission² "*Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems.*"

The biggest threat in facing cybercrime is given by the borderless nature of the problem. Indeed, it is widespread and hardly circumscribed to a specific geographical area or specific actors. Cybercriminals may both act individually or as a group, and the possibility of perpetrating a cyberattack from anywhere makes it harder to control and prevent them and at the same time make it easier for cybercriminals to start a cyber-incident. Moreover, the lack of a diffused digital culture through the population and corporations enhances the probability of occurrence of a cyber-incident and its severity. Besides, the more severe the consequences of a cyber-attack, the more expensive it will be for corporations and institutions to cover the damages.

The sources of costs arising from cyber-attacks comprehend costs of different nature. The majority of the costs are given by monetary costs, which is the amount of money necessary to solve technical problems arising from the attacks. Moreover, we have also direct costs linked to the amount of money stolen by cybercriminals. This amount differs between different industries, for instance, the monetary impact is certainly higher for those activities, such as the one carried out by Financial Intermediaries, which strongly rely on the functioning and efficiency of their ICT infrastructures.

² Source: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

Furthermore, we have to take into consideration reputational costs. These costs have an important impact specifically on banks, financial intermediaries, and all the actors of the financial system. The soundness of Financial Intermediaries and the trust of business and retail clients in the financial system is fundamental for their stability. In particular, reputational costs mostly arise from a Data breach attack, in which data of different natures, such as private data about the company's strategies or personal data about customers, are illegally acquired by cyber-criminals.

Nevertheless, each kind of attack can give rise to reputational damages. This kind of damages may lead to different sources of costs:

First of all, for what concerns direct reputational costs, according to Ronchi³ we have to consider all those costs needed to restore the original reputational state through a reputational campaign. Then, we have the loss of earnings, since some clients may decide to terminate their contracts with the institutions that have been breached. And finally, we have the loss of new clients and opportunities related to the lower attractiveness towards new potential clients, which will opt to rely on different institutions, hence lowering the firm market share compared to competitors. Moreover, another family of costs arising from cyber-attacks is opportunity costs, which can be seen as the amount of time needed to solve technical issues linked to a cyber-attack, and as the amount of money spent and not invested in profitable investing opportunities. Every day spent in solving technical consequences related to the attack will lead to the impossibility of engaging in productive investment opportunities and to an inefficient channeling of funds.

The average cost in terms of time of a malware attack is **50 days** but varies according to the industry and the severity of the cyber-attack consequences⁴.

To give an idea of the importance and the growth of the phenomenon we are going to analyze some data coming from the 2020 Clusit Annual report on ICT security in Italy⁵. This report is based on the analysis of **10.938** cyber incidents of public domain that occurred in Italy between 2011 and 2020.

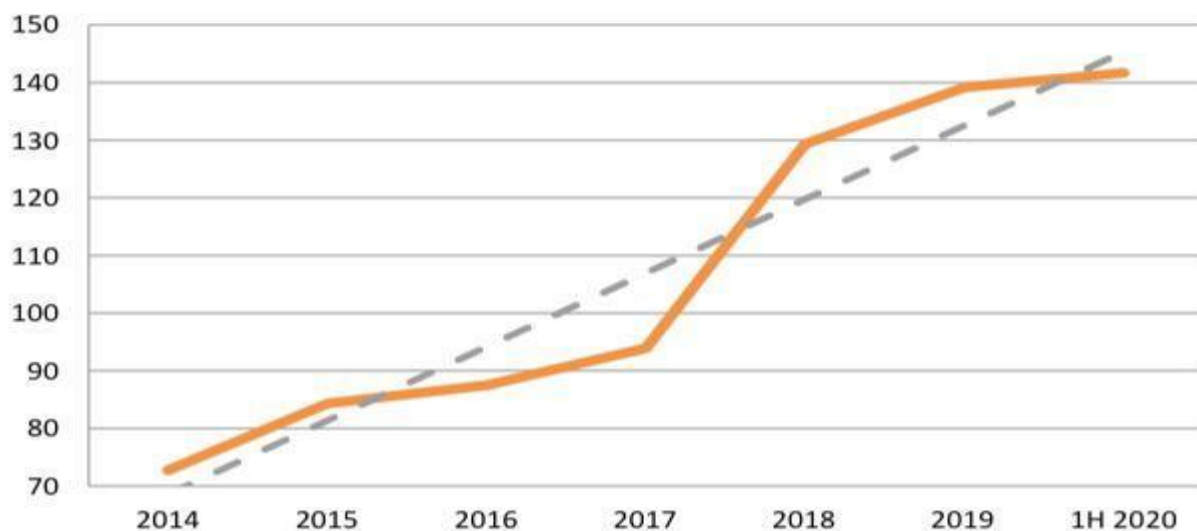
³ Ronchi, A., (2018), Come si calcola il danno reputazionale?

⁴ Source: <https://purplesec.us/resources/cyber-security-statistics/#>

⁵ Clusit, (2020, Clusit Annual Report 2020

In particular, the sample is made of cyber-attacks considered of high severity which had a significant impact on the victims in terms of reputation, economic losses, and data breaches. Moreover, **1670** of those cyber-attacks were perpetrated in 2019 and **850** in the first semester of 2020. Furthermore, the trend of the monthly average of cyber-attacks in the last six years has increased by **91.2%**.

Figure 1: Average of relevant attacks per month



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - aggiornamento giugno 2020

Source: Clusit Annual Report 2020

It is important to underline that the Clusit Annual report takes into account only some cyber-attacks and that the number of attacks occurring every day in Italy and all over the world is way bigger. Moreover, the scarcity of precise and certain data is also due to the submissiveness of the various targets, which in most cases are reluctant to admit that they have been hit by a cyber-attack.

Also, the spread of Coronavirus in the whole world has worsened the situation. In fact, by moving day-by-day activities such as working and education into cyberspace, the amount of traffic has increased tremendously giving cyber-criminals a wider range of options and targets. According to a report published by Panda Security⁶, one of the biggest players in the Antivirus sector, Internet scams grew by **400%** in March 2020, making COVID-19 the largest security threat ever, while in April Google blocked more than **18 million** daily malware and phishing attempts.

Furthermore, in regards to remote working, the level of cyber-defense tools of personal computer devices and private connection IP addresses is, in most cases, definitely lower than tools used by workers in corporate offices. Thus, in some cases, the pandemic enhanced the power of cybercriminals to such an extent that with the COVID-19 pandemic we have seen the development of a cyber-pandemic.

⁶ Source: <https://www.pandasecurity.com/en/mediacenter/news/covid-cybersecurity-statistics/>

1.3 CYBER-ATTACKS IN THE FINANCIAL SECTOR

As the Federal Reserve President Jerome Powell stated in his appearance before the House Financial Services Committee on August 9th, 2018⁷, cybersecurity and the unexpected dangers therein included are the biggest threat to the financial system. According to his vision, banks and financial intermediaries should prepare for the worst-case cybersecurity scenario, giving this issue greater importance than the one given to traditional risks. Therefore, the financial sector should strongly focus on preventing and preparing for these kinds of threats. Moreover, he added that the Federal Reserve takes the supervision of banks seriously, and advised them to continually maintain basic cyber hygiene, by keeping their cybersecurity system up to date on emerging trends and threats coming from cyberspace usage.

Even though the Federal Reserve is doing as much as possible to prevent bank failures it is impossible to predict what would precisely happen in case of a successful large-scale cyber-attack, and the whole system must have an emergency plan. In particular, all these concerns are due to the fact that the banking and the financial sectors must adapt promptly to changes in the cyber-environment to guarantee maximum efficiency and continuity to those services considered essential in the financial sector.

The role and the functioning of the banking and financial sector circuits are fundamental for the correct and smooth functioning of the economy, and any vulnerability can be exploited by the different actors which are active in the world of cybercrime.

⁷ Lowary, J., (2018), Three Important Things Jerome Powell Said to Congress

Cybercriminals in most cases act for a monetary purpose, acting both on their own or in organized groups. The number of active cybercriminals is increasing, and to understand the threat posed to the stability and efficiency of the financial system as a whole is important to identify them:

- 1) Hackers** are the most famous category of cyber-criminals. They might use their skills only to mock their targets or to acquire notoriety in their environment. Only some of them exploit their knowledge in order to benefit from their activities. According to Vitagliano Stendardo A. ⁸*“hackers deeply believe that information is the heritage of humanity, and should be used to improve the conditions of the community”*. Hackers tend to think that information is being filtered and exposed by governments, enterprises, and financial institutions to gain profits and protect their interests, and always according to Vitagliano Stendardo A. ⁹*“as a reaction, some hackers feel legitimated to penetrate systems, not to block or damage them, but to recover and diffuse what everyone has always been entitled to”*.
- 2) Crakers** are those cybercriminals who want to penetrate private and public systems of targets to damage them. They can be considered as a more dangerous category of hackers.
- 3) Hacktivist** is the term used to indicate a category of subject active in the so-called Cyber-hacktivism. They are driven by ideological motivations. A famous example of Hacktivist is the Anonymous group.

All those actors are active in the cyber environment and use different kinds of cyber-attacks based on their objectives.

⁸ Vitagliano Stendardo, A., (2010), La criminalità informatica nei sistemi di pagamento digitale e con smart card. First edition. Gedit Edizioni. Bologna. (p.104)

⁹ Vitagliano Stendardo, A., (2010), La criminalità informatica nei sistemi di pagamento digitale e con smart card. First edition. Gedit Edizioni. Bologna. (p.104)

The most common Cyber-attacks in the financial sector are:

- 1) Malware** that according to the Clusit annual report 2020¹⁰ is the most common technique of attack, making on their own almost half of the cyber-incidents analyzed, precisely **44%**. The malware is a dangerous software designed to access a computer system without the consent of the owner. In this category are included the well-known viruses and ransomware, through which hackers limit the access to a computer system asking a ransom payment to unlock it¹¹.
- 2) Data Breach**, which according to the United Kingdom information commissioner Office¹² is a cyber-incident in which sensible, protected, confidential and personal data are stolen, altered, disclosed, and in some cases also destroyed.
- 3) DDoS**, which means Distributed Denial of service. This is a dangerous attack since its target is to make a service non-usable. It has criminal purposes, such as a monetary return. Due to the interruption of services, the attacked institution will incur economic losses, and in particular in the financial sector, it could also have a greater impact on the system as a whole.
- 4) Phishing** is one of the most common frauds that concerns consumers. It consists of the illegal acquisition of personal data registered on the internet for the conduct of online services such as access to personal banking platforms and services. In this type of attack, fraud is committed through the creation of fake websites, which will mislead consumers and businesses. According to an article by Lombardo on Cybersecurity360¹³, the number of phishing attacks has significantly increased during the Covid-19 pandemic.

¹⁰ Clusit, (2020), Clusit annual report 2020

¹¹ Source: <https://www.avast.com/it-it/c-ransomware>

¹² Personal data breaches, UK Information commissioner's Officer

¹³ Lombardo, S., (2021), Cyber crime, aumentano attacchi informatici e truffe online a tema Covid-19: come mitigare i rischi

5) Social engineering techniques, which are all those techniques aiming at understanding the behavior of web users and exploit their vulnerabilities to acquire useful information such as credentials for online services.

The Financial sector is one of the most attractive for cyber-criminals due to the valuable nature of its assets and the exchanged and private business information. Moreover, it focuses on the movement, exchange, storage, and protection of the primary target of cybercriminals, money. The evolution of crime in the financial sector has moved in parallel with the evolution of cyberspace and its usage for business and financial purposes. Even though bank robberies still occur, nowadays they are not the primary concern for banks.

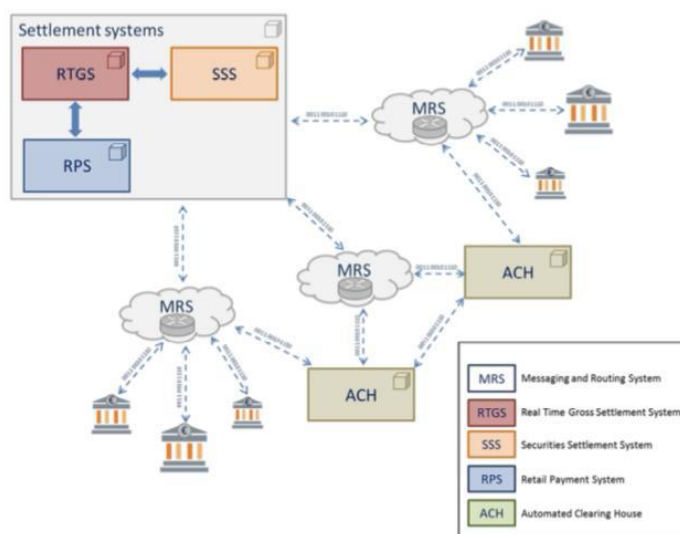
Cybercrime has raised more concerns than standard crime since it is more difficult and costly to prevent, it can occur anytime and from anywhere and it is always evolving, thus making necessary continuous and growing investments in cyber-security measures and formation. Furthermore, as we are going to analyze more in-depth later on in our analysis, the growing interconnection of the financial intermediaries of different countries poses a serious threat to the stability of the economies around the world. The dangerousness of cyber-threats in the financial sector is given by the fact that a cyber incident could spread rapidly and affect a great number of institutions.

One of the most common targets in financial cybercrime is the Interbank payment system, which is used to assist banks in settling transfers of money and information between financial intermediaries. In particular, the system used by financial intermediaries to communicate with each other is the **MRS**, the messaging and routing system. Cybercriminals try to enter in the process of transmission of the codes in order to intercept the funds transferred by banks and take possession of large amounts of funds. This is the case of the case study that will be presented in the second chapter concerning Cosmos bank, and also of other famous cyber-attacks such as the recent attack against the central bank of Bangladesh, that resulted in a monetary loss **of \$101 Million**¹⁴.

¹⁴ Source: https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery

According to the occasional paper published by Fazio and Zuffranieri in 2018 for the Banca D' Italia¹⁵, each transaction occurring in the MRS has a recognizable code that identifies the beneficiary's bank. The codes are conveyed through a system used to manage the transmission and reconciliation of payment orders and calculate the final balance to be settled, the Automated clearing house. Different kinds of payments are settled through different systems (RTGS for large value transactions, RPS for retail transactions, and SSS for the exchange of securities). To enhance trust in this payment system accounts used to settle transactions are opened at central banks. It is important to underline that the MRS transmit only messages, and the actual transactions are settled only through the accounts opened at central banks.

Figure 2: MRS role in the domestic payment system



Source: www.bancaditalia.it QEF 418

Furthermore, the MRS is used to settle international payments with similar procedures. In this case, a few differences arise when the payments have to be settled among countries that do not share the same infrastructures and procedures. The international MRS functions as a center where all the transactions are routed.

¹⁵ Fazio, A., Zuffranieri, F., (2018), Questioni di Economia e Finanza, Occasional Paper for the Bank of Italy, Interbank payment system architecture from a cybersecurity perspective (pp 6-8)

While at the national level we have different but interconnected MRS, for what concerns international payments the smooth functioning of the MRS has greater importance since it connects all the players, so the slightest problem in its functioning could potentially cause trouble to institutions all over the world.

For international payments it is necessary another system in addition to the RGS, RPS, and SSS, the MSS (Multi-Currency settlement system), which is needed to settle transactions with different currencies. In this case thanks to a central Hub such as the International MRS, banks can also settle payments directly, with binary transactions, without passing through different central banks. Cybercriminals try to enter in this process to intercept payment codes as further analyzed in the last chapter in a case study about the Cosmos Bank heist fraud. In particular, **SWIFT** is the only company acting as an international MRS worldwide.

A common target is customers with their personal data, such as Internet and Mobile banking credentials and credit card credentials. In fact, according to the ABI 2017 annual report¹⁶, during 2016 the **0,45%** of retail clients using internet banking have undergone credentials theft, and **0,0141%** have suffered a monetary loss. On the other hand, for what concerns corporate customers the percentage of clients that have undergone credentials theft is **0,67%**, while only **0,0054%** have suffered a monetary loss. These data show how much importance is given to this phenomenon and that banks are increasing their level of attention year after year to minimize losses for their clients, which have the right to be reimbursed.

Always according to ABI annual report published in 2017¹⁷, retail clients are the preferred target of cybercriminals as they are subject to **70,4%** of the cyber-attacks, while **68,8%** of illegal transactions have been carried out from the corporate clients' segment.

The main objectives for financial cybercriminals remain the acquisition of credit card data and payment system credentials along with the change of payment coordinates.

¹⁶ ABI Lab, Cert Finanziario Italiano, (2017), Sicurezza e frodi informatiche in banca: come prevenire e contrastare le frodi su Internet e Mobile banking

¹⁷ ABI Lab, Cert Finanziario Italiano, (2017), Sicurezza e frodi informatiche in banca: come prevenire e contrastare le frodi su Internet e Mobile banking

Although the impact of credit cards fraud may seem less relevant from a macroeconomic point of view, due to the increasing trend in their usage has to be considered as a primary threat, in fact, according to the Finance Focus by Rotondo in the Clusit Annual Report 2020¹⁸, during 2016 the total of fraudulent transactions that occurred in the SEPA region amounted to **€1,8 billion**.

The focus on cybercrime against payment infrastructures is of increasing importance nowadays since central banks are starting to think about the issuance of Central bank digital currencies (**CBDC**). Central banks, driven by the tremendous increase in usage of Cryptocurrencies and by the need for innovation, view the creation of CBDC as a tool to give citizens new and less risky means of payments. CBDC would be the response given by Central banks to the increase in cryptocurrency circulation.

The total market capitalization of Cryptocurrencies reached during 2020 the astonishing amount of **\$758.06 billion** according to a publication of de Best on Statista (2021) in which he analyzed the evolution of the Cryptocurrency Market Capitalization between 2013 and 2020¹⁹. In this contest, the issuance of CBDCs would broaden the means of payment available. A concrete example of CBDC is the digital euro, which is currently being studied by the ECB. This digital currency is seen as a possible alternative to standard means of payment and as less volatile and safer than cryptocurrencies, as stated in the Report on digital euro published by the ECB in October 2020. Even though CBDCs appear to be less risky than other cryptocurrencies the ECB needs to focus on the cyber resilience of the critical infrastructures needed to make it work since an attack directed to CBDC infrastructures could have a disastrous impact on the financial system.

Moreover, another important and common target for cybercriminals is financial markets, with particular regard to the stock market. The efficiency of stock markets could be hampered by DDoS attacks, attacks blocking completely the functioning of the concerned infrastructure, as happened in New Zealand where on the 25th and 26th of August 2020 the **NZX exchange** was interrupted by several cyber-attacks²⁰.

¹⁸ Rotondo, P.L., (2020), Clusit annual Report 2020, Finance focus (p. 103)

¹⁹ De Best, R., (2021), Cryptocurrency Market Capitalization 2013-2020

²⁰ Farrer, M., (2020), New Zealand stock exchange hit by cyber attack for the second day

Another possible cyber incident was prevented in 2010 when hackers managed to breach Nasdaq's cyber defense tools and place a malware, which could have possibly spied on to steal precious and sensitive information and data if not detected. Cybercriminals may attack stock markets for demonstrative purposes, or to disrupt the confidence in the correct functioning of financial channels. The latter objective is usually pursued by those cybercriminals backed by states that profit from the disruption of the economic activities of eastern countries, such as North Korea.

Non-bank financial institutions such as wealth management funds, mutual funds, and insurance companies are other sensitive targets due to the amount of private information stored in their systems, including customer's names, social security numbers, payment and credit card data, and other personal information. Acquired information can later be sold in the black market, where there is a high demand for such information to be used for identity fraud.

To understand why financial companies are working under constant pressure it is important to underline some aspects of cybercrime in the financial sector:

As stated by Verizon in the 2020 data breach investigations report, financial services are usually hit harder by data breaches than companies in other industries, with an average of **352,771** exposed sensitive files, while other industries expose on average **113,491** files²¹. Moreover, the banking sector has on average the highest cost from cyber incidents, with an average of **\$5.85 million** per data breach and **\$18.3 million** for other typologies of cyber-attacks. Lastly, while the average amount of days to detect and contain a cyber-attack is **55 days**, for financial services it takes an average of **233 days** to detect and contain a cyber-attack²². Moreover, Accenture has estimated a loss in value of **\$5.2 trillion** for the period 2019-2024 across all industries, while banks are expected to lose **\$347 billion**, insurance companies a total of **\$305 billion**, and capital markets **\$47 billion**²³.

²¹ Verizon, (2020), 2020 Data Breach Investigations Report

²² Sobers, R., (2021) 134 Cybersecurity Statistics and Trends for 2021

²³ Accenture security & Ponemon Institute LLC, (2019), The cost of cybercrime







According to this prediction and due to the worsening of the caused by the COVID-19 spread all over the world, in an article written for Deloitte & Touche LLP and the Financial Services Information Sharing and Analysis Center, Bernard and Nicholson²⁴ estimated that spending on cybersecurity in the financial sector rose by **15%** from 2019 to 2020. The average spending per employee increased from **\$2,337** in 2019 to **\$2,691** in 2020 with some financial intermediaries expecting to spend more than **\$3000** per employee. The spending varies for firms of different sectors active in the financial industry.

Table 1: Cybersecurity spending across sectors

FIGURE 2

Cybersecurity spending across sectors

■ Percentage of revenue ■ Percentage of IT spending ■ Per FTE

		2019	2020
	Retail/corporate banking	0.3% 10.1% US\$2,074	0.6% 9.4% US\$2,688
	Consumer/financial services (nonbanking)	0.3% 9.7% US\$2,817	0.4% 10.5% US\$2,348
	Insurance	0.3% 9.3% US\$2,245	0.4% 11.9% US\$1,984
	Service provider	0.6% 8.9% US\$1,956	0.6% 7.2% US\$3,226
	Financial utility	0.8% 15.2% US\$3,630	0.8% 8.2% US\$4,375
	Aggregated total	0.3% 10.1% US\$2,337	0.5% 10.9% US\$2,691

Note: FTE=Full-time employee or equivalent.

Source: www2.deloitte.com/us/en/insights.html

FS-ISAC/Deloitte Cyber & Strategic services CISO survey reports 2019-2020, Deloitte center for financial services

²⁴ Bernard, J., Nicholson, M., Deloitte and FS-ISAC survey, (2020), Reshaping the cybersecurity landscape

CHAPTER TWO

The Economic consequences of cyber attacks

2.1 THE ECONOMIC IMPACT OF CYBER ATTACKS IN THE FINANCIAL SECTOR

As introduced in the first chapter, cyber-attacks can have a serious impact on the stability and soundness of the financial sector. Several studies and speculation have analyzed the actual and possible impacts of cyber incidents over the different components of the financial environment. Some of the consequences are proved by studies, such as the impact over the stock prices of different companies after the occurrence of a cyber-attack is made public, while others are only hypothetical since a lot of cyber incidents have not been detected yet. Also, the amount of available data is not sufficient to give an exhausting analysis of all the consequences of cyber incidents, partly because cyber threats are always evolving and targeting new vulnerabilities.

Both Christine Lagarde and Jerome Powell have underlined the importance to guarantee the protection of critical assets and information several times to ensure the stability of the financial infrastructures. The actual president of the ECB warned that according to a report of the **European Systemic Risk Board** (ESRB), the global cost of cyber-crime is estimated between **\$45 billion** and **\$645 billion**²⁵. Miss. Lagarde also stated that financial channels are plausible channels that could lead a cyber-attack to cause a more serious financial crisis. In particular, it has been theorized that a Distributed Denial of Service attack causing an operational interruption by damaging or encrypting the balance accounts of important financial intermediaries and institutions, could lead to a liquidity crisis.

²⁵ Winder, D., (2020), \$645 Billion cyber risk could trigger liquidity crisis, ECB's Lagarde warns
Source: <https://www.forbes.com>

The ESRB report²⁶ analyzes how the liquidity crisis caused by a financial attack could escalate and lead to a systemic crisis. According to the analysis, cybersecurity is crucial to prevent a higher systemic risk, the risk of disruption in the financial system, that could potentially have dangerous repercussions for the internal European market and the real economy. The increase of a diffused cyber resilience in the financial markets is needed to guarantee financial stability, that is the appropriate functioning of financial markets and intermediaries in support of the real economy, needed to guarantee the capacity to absorb external shocks and to continue providing the essential economic functions also during these shocks.

As we know from the previous economic crises, financial stability is threatened when financial markets cannot absorb shocks, and in this case, unfavorable situations such as liquidity and lending freezes, bank runs, market crashes, and also hyperinflation could occur. Moreover, the evidence from past financial crises tells us how uncertainty and loss of confidence in financial intermediaries can incentive crises and trigger financial instability. Particularly, it is important to take into account that situations of instability are caused both by direct actions of financial market intermediaries and participants in response to a shock, such as a situation of insolvency of an important financial institution or by an important fall of public confidence on the soundness of specific intermediaries and the financial market as a whole.

Other important factors are the size of the initial shock and the transparency of the intermediaries about the losses incurred during a shock. Even though a cyber-attack capable of disrupting financial stability hasn't happened yet, the operators of the financial system need to be aware of this possibility and take into consideration also the worst-case scenario. In fact, even though not every cyber incident represents a danger to financial stability, it remains possible that in the future a broader-scale cyber-attack could create a situation of disruption and cause negative effects for the economy as a whole.

²⁶ European Systemic Risk Board, (2020), Systemic cyber risk

The ESRB has also developed a conceptual model to analyze if a cyber incident could become a systemic risk. There are four factors to be taken into account:

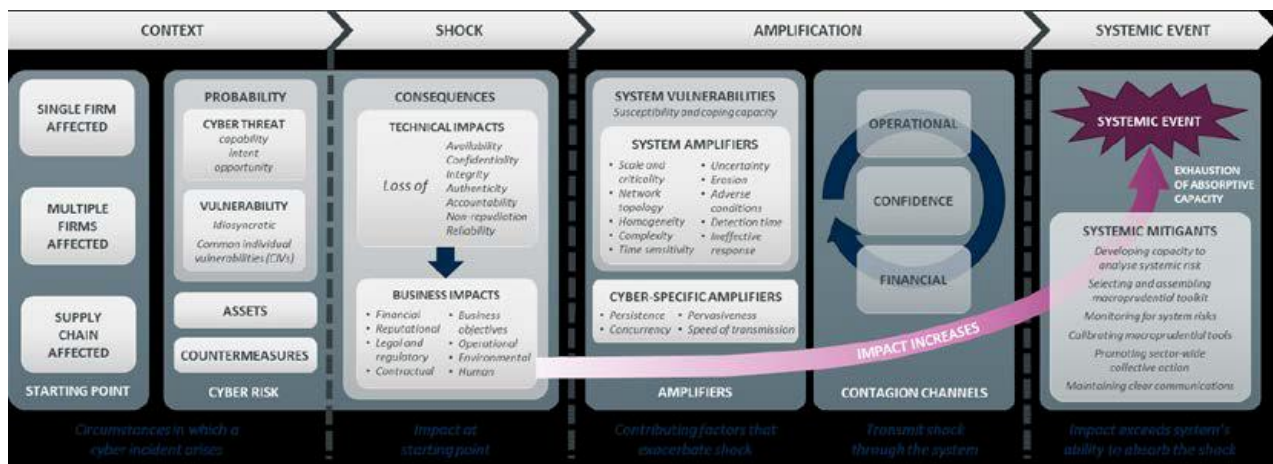
- 1) The **context** can be considered as the actual starting point of a cyber incident. The first aspect to be analyzed is the number of firms affected by the cyber incident since it will be easier to isolate single entities and prevent the propagation of the damage caused by the cyber-attack. In the case of multiple entities, it is important to have a common approach to the resolution of operational and confidence problems. The second part of the context phase comprehends the analysis of the cyber threat, taking into account the **capability**, which is the ability of the criminals to achieve their intended objectives, the **intent**, that is the degree of involvement of the threat actor in causing the harm to the affected entity, and the **opportunity**, the timing of the attack and knowledge of cybercriminals of the target firms with its vulnerabilities. An analysis of the vulnerabilities is necessary to ascertain if it pertains to the single firm or if it can be considered a diffused vulnerability, for example, if it is part of a technology used by different firms. Then the assets affected have to be analyzed and in case of financial resources quantified, with the countermeasures that the firm has adopted.

- 2) The **shock** takes into account the consequences caused, directly or indirectly, by the incident. It aims to understand what are the specific technical impacts, the immediate negative effects on the assets affected, such as the loss of **availability** of the information systems, the **integrity** of data, and the **reliability** of the institutions affected, that can, later on, affect the broader economic environment. Then it analyzes the business impact, such as the **financial losses** caused by the incident, the negative **brand damage**, causing reputational issues, a reduced level of services provided and legal, regulatory, and contractual problems arising from the breach of contracts and obligations between the firms and its client/customer.

- 3) The **amplification** describes how the impacts affecting a single institution can be transmitted to the whole financial system. It is important to analyze the system vulnerabilities that could lead to a spillover of the contagion, such as the system amplifiers, those aspects that can lead to a disruptive evolution of a single incident. Those factors include the **network topology**, the **level of interconnections** with the other institutions, that for the financial system is usually high enough, the **detection time**, and the **effectiveness of the response**. Then some aspects are considered cyber specific amplifiers, those characteristics which are specific to cyber incidents, such as the **speed of transmission** of the operational and reputational damage, the **persistence** of cyber-attack and the **concurrency**, the ability of a cyber incident to create a diffused and compound shocks through the use of different vectors and techniques of attack. Then it analyzes the contagion channels, divided into three categories. The **operational channel**, which comprehends the spread of operational damage to different institutions, that can be caused by Distributed Denial of Service attack, the **confidence channel**, which takes into account the ability of a low level of trust of customers in the financial institution affected to spread to others institutions that otherwise wouldn't be affected, and the **financial channel**, that takes into account the possibility that the huge financial losses incurred by a firm could lead to the propagation of risk on the whole financial system.
- 4) The **systemic event**, that is the risk of disruption to financial services caused by the inoperability of a part of the financial system following a serious cyber incident and that has the potential to affect directly, with negative consequences, the real economy. In order to avoid a situation of systemic crisis, the supervisors should set some **impact tolerance thresholds**, considered as the maximum impact that the financial system can tolerate without experiencing a systemic crisis. Each firm, to avoid such a situation, should respect the minimum requirements threshold, that can be applied to develop an adequate level of cybersecurity and detection of the impacts of a cyber-attack.

These four factors, each representing a step of the analysis, are well defined in the following scheme developed by the ESRB in one of its occasional papers, “*The making of a cyber crash, a conceptual model for systemic risk in the financial sector*” published by Greg Ros in May 2020. The model developed by Ros²⁷ can be used to deconstruct and describe the macro-financial implications of the risk arising from cyber incidents, and to analyze both hypothetical and past scenarios that actually occurred. It aims at giving additional resources to financial firms for a deeper understanding of cyber threats and their actual and possible impact.

Figure 3: The four phases of the systemic cyber risk model



Source: Occasional Paper Series, No 16/ May 2020, ESRB

The ESRB theorized the impact of different hypothetical scenarios on the financial system to understand the possible consequences, following the four phases model presented. For example, the board analyzed what would happen in case of incapacitation of a large domestic bank’s payment system. Banks are fundamental contributors to retail payment systems. What would happen in case of an interruption of the software operations of a bank?

²⁷ Ros, G., European Systemic Risk Board, (2020), Occasional Paper Series No. 16

Context Phase: A bank controlling various payment processing systems is attacked, and the attack corrupts all payment data in the bank's system.

Shock Phase: As the payment processing system does not run correctly for a while, millions of transactions of both retail and business clients cannot be processed. The account balances of the bank will be unavailable for the whole duration of the incident. The bank is facing operational problems and has to stop its retail operations. This action will have also a strong impact on the reputation of the business. The short-term financial impact will be contained, but the long-term financial impact will be harsher. The long-term costs will comprehend fines, customer losses, and loss of market share in favor of its competitors. Moreover, there are possible technical impacts, given by the complex process of reconciliation of the operational activities, which lead to concerns for the integrity of personal data.

Amplification phase: The unavailability of account balances affects drop-down all the business activities and services relying on the availability of account balance information. These activities include debit and credit cards transactions, mobile and online banking, and also cash withdrawal. In this stage, the cyber incidents start to affect also the counterparties, since payments from customers to third parties and businesses cannot be settled. Customers cannot access their balance accounts and start doubting the soundness of the financial institution. For this reason, insolvency becomes a further concern. As the news of the incidents goes public, the bank stock's prices decrease. The bank will have to pay higher risk premia, and due to the high interconnection between financial intermediaries, the spillover effects lead to an overall increase in uncertainty towards the financial system. The consequences for the customers become harsher as time passes, and the spillover of uncertainty affects the cost of borrowing and lending of all the actors of the financial system, leading to an increase in Moral Hazard and Adverse Selection. Due to asymmetric information, customers of competitors institutions start fearing to be in the same situation as the affected bank.

Systemic event: In this hypothetical scenario, the operations of the affected bank are completely shut down. The prolonged disruption of the operational capability of the intermediary and the spread of concerns and uncertain news could be the triggers of a larger scale financial instability, causing liquidity problems and bank runs. The self-fulfilling nature of the spread of concern and disappointment towards the financial industry's resilience and stability contribute to increasing systemic risk. The possibility of insolvency of a single financial institution can be fatal for the financial sector as a whole, as we know that situation of distress usually starts from a single institution and then spreads to the broader industry.

Even though the previous case is only a speculation, it represents a good approximation of possible economic consequences of cybercrime in the financial sector. Due to its nature of systemic risk, cyber risk can be compared to any source of operational risk. According to the Federal Reserve Staff Report No.909²⁸, two characteristics distinguish this kind of risk from the others. When a firm is subject to a cyber incident, the security and integrity of private data and information cannot be guaranteed. Moreover, the ability to guarantee the bank services is impaired, rendering the first-mover advantage useless. Even though the bank could in theory concede the requested liquidity, in some cases it is not able to run the services needed to practically distribute the money, since its operations are blocked. But the unusual nature of the attack and the ensuing uncertainty may prompt bank runs to occur in other segments and institutions that otherwise wouldn't be affected.

According to a paper by Martin Boer and Jaimie Vazquez of the Institute of International Finance²⁹, the measures applied after 2008 to prevent the failure of large financial institutions and to protect the financial system from systemic risk cannot be applied to address the core factors of cyber-risk.

²⁸ Eisenbach, T. M., et al, (2020), Federal Reserve Staff Report No.909, Cyber Risk and the U.S financial System: a pre mortem analysis

²⁹ Boer, M., et Al, (2017), Institute of international finance, Cybersecurity & Financial Stability: How cyber-attacks could materially impact the global financial system

The reform to safeguard the financial system, asking greater capital and liquidity requirements to financial institutions, do not take into account that cyber-attacks could impact the system not only directly, through a single institution and different components of the financial sector at the same time, but also indirectly through the impact of cyber-incidents on the providers of essential services such as electricity and telecommunications. For example, in the latest years, subsea telecommunications infrastructures are becoming fundamental for the correct functioning of international communications.

According to the paper of Lionel Carter³⁰ et al., "*Submarine cables and the oceans: connecting the world*", already in 2009, **90%** of global telecommunications and traffic data passed through the undersea wiring. For this reason, these infrastructures are acquiring growing importance for sectors such as the financial one, where data and communication take part in the process of value creation

For instance, these infrastructures are crucial for the correct functioning of the **SWIFT** systems, which manages daily communications for the interbank payment systems for almost all the financial institutions. An attack limiting the correct functioning of the SWIFT systems may cause great concerns for the stability of financial institutions, increasing the systemic risk and leading to a possible liquidity crisis.

Also, the **ICE**, the **Intercontinental Exchange**, which manages a global network for the forex market and daily processes millions of futures contracts on commodities and financial derivatives on the over-the-counter market, bases its activities on the stability and smooth functioning of the subsea infrastructures.

Therefore, the progressive dependence of the economic and financial activities on electronic and transoceanic communication is further becoming a possible target for those cybercriminals aiming at disrupting the economic stability, both for personal advantage and for political reasons.

³⁰ Carter, L., et Al., (2009), *Submarine cables and the oceans: connecting the world*

In order to quantify the risk faced, the ESRB employs a model of probabilistic risk assessment, developed by Norman Rasmussen in 1975, to capture the main determinants of cyber risk³¹:

$$\text{Cyber risk} = \frac{\text{cyber threat} \times \text{vulnerability} \times \text{assets} \times \text{consequences}}{\text{Countermeasures}}$$

This model takes into account the level of the current cyber threat, the vulnerabilities present in the systems of interest, the value of the assets involved, both tangible and intangible, and the consequences of cyber-attacks, using countermeasures as a deterrent. After having suggested a measure to quantify the cyber risk, the ESRB focused on the measurement of the impact of various incidents. First of all, it identified different types of impacts, such as the direct financial impact, which comprehends financial and monetary losses due to fines, penalties and forgone profits for the loss of market share of a specific financial intermediary, and the reputational impact, that has to do with the negative opinion and brand damage affecting the financial intermediary and in most alarming cases the whole financial industry, amplifying the systemic risk. Furthermore, contractual and legal impacts need to be taken into account. After identifying the different kinds of impacts affecting financial operators, the ESRB focused on the measurement of the impact. The measurement of business impacts over individual financial institutions can be decomposed by using two complementary approaches:

- 1) A **qualitative** approach, which is judgment-based and uses descriptive statements to describe levels of increasing harshness for the different categories of impact. This qualitative approach is mainly used to guarantee and drive an adequate organizational response. It is the most common approach since it is easier to define and implement, even though it is based on the arbitrary judgment of individuals, which can lead to bias in the measurement of the impact. In fact, people who are responsible for cybersecurity of a company may be tempted to downplay the actual impact of a cyber-incident to avoid heavier consequences.

³¹ Ros, G., European Systemic Risk Board, (2020), Occasional Paper Series No 16

- 2) A **quantitative** and metric-based approach, that makes use of data-driven indicators to calculate different degrees of impact. It is more difficult to employ since it requires an accurate definition and search of timely data to use in order to prepare the organizational response.

The different kinds of impacts vary across time horizons. For example, in the short run firms should focus on operational impacts, such as business service disruption and the downstream impact on the services offered by the institutions.

If the institutions manage to overcome the operational consequences and to guarantee operational continuity, reputational and financial impact may be contained. For financial stability, it is important to look at long-run indicators, and if the perceived business risk is protracted over time, the decrease in confidence over the specific intermediary and the financial industry as a whole may lead to a situation of systemic risk.

Figure 4: Potential impact indicators of cyber-attacks

Category	Measurement subject	Potential impact indicators	Horizon
Financial	Incident related expenditure	Costs incurred to handle the incident (e.g. technical investigation, return to normal operations, public relations)	Short
	Customer detriment	Costs incurred for incident notification, customer protection, financial reimbursement	Short to Medium
	Deposit stability	Measuring deposit rates and flows over time, e.g. Liquidity Coverage Ratio (LCR)	Short to Medium
	Market value	Stock valuation using Cumulative Abnormal Returns (CAR)	Medium to Long
	Profitability ratios	Gross/net profit margin, EBITDA, Return on Equity (ROE)	Medium to Long
	Perceived business risk	Costs for raising debt relative to credit rating, change in insurance premiums	Medium to Long
	Loss of competitive advantage	Value of lost contract revenue or loss of intellectual property	Long
	Regulatory costs	Fines or fees levied for non-compliance	Long
	Capital charges	Pillar II capital add-on	Long
	Litigation	Penalties for breach of contract, settlement costs	Long
Confidence	Media coverage	Negative news signals, volume of attention, adverse social media activity, reputation index, number of press enquiries	Short to Medium
	Investor sentiment	Market-based measures (e.g. CBOE Volatility Index) and technicals (e.g. Relative Strength Index, Money Flow Index)	Short to Medium
	Brand valuation	Customer surveys for top-of-mind awareness, familiarity, advocacy	Medium to Long
	Customer metrics	Measuring customer satisfaction, loyalty, acquisition, retention, problem incidence	Medium to Long
Operational	Business service disruption	Trading volumes and values, service availability, performance indicators	Short to Medium
	Downstream impact	Number of dependent services disrupted, number of third parties / customers affected	Short to Medium

Source: ESRB Occasional paper series No. 1

It is always important to underline that the actual impact of cybercrime on the economy is difficult to quantify. In fact, not every cyber incident is discovered, and of those that are known by the affected institutions, only a small part is disclosed, to avoid reputational consequences that can lead to a deeper impact, both for the institution and for the economy. For example, data leaks are growing both in their incidence and in the possible impact that may arise. The increasing amount of data stored by institutions of all kinds is a precious target for cybercriminals. These attacks cause irreversible damage to the affected companies such as financial intermediaries, that store and protect sensitive data of all kinds, from personal data such as names, addresses, and fiscal codes, to financial data. They store the records of every transaction, the balance account of each retail and business customer, payment credentials, and credit card credentials but also company private data such as internal communications. Furthermore, with the evolution of electronic and online banking, the amount of stored data increases exponentially day by day, enlarging the scope of action of cybercriminals.

United States companies face the highest average cost of data breaches, that according to the report regarding the cost of data breaches in 2020 published by IBM in collaboration with the Ponemon institute amounts to **\$8.19 Million**³². However, financial companies are more concerned about the related risk arising from data breaches, which can cause a fall in the confidence in the financial system, which in turn may lead to a situation of systemic risk. For this reason, legislators and supervisors are constantly collaborating with financial institutions to increase their resilience to that kind of attack.

One of the economic factors most affected by cybercrime is certainly the stock value of a company. According to the paper "*Stock market cybercrime*" Published by Alexandre Neyret³³, there are mainly three kinds of stock breaches: Insider trading, price manipulation, and dissemination of false or misleading information. The financial impact of cybercrime varies according to the damage caused by the attack and to the kind of attack suffered.

³² IBM and Ponemon Institute, (2020), Cost of a Data Breach Report 2020

³³ Neyret, A., (2020), Stock market cybercrime

Ros³⁴ in its report for the European Systemic Risk Board has analyzed the potential impact on the market of a price feed manipulation concerning commodities and futures market, using the framework developed by the ESRB to analyze actual and hypothetical scenarios following a cyber-attack. In the context phase, multiple firms would be affected, such as market data providers and Central Counterparty Clearinghouses, entities active in the European trading and derivatives markets as a facilitator of the operation between buyers and sellers. The Hackers could enter into the system by using a malicious code inserted in the financial infrastructure used to process the actual prices and the last trades, to select and modify the information received and sent out by the systems. This situation leads to a loss of reliability of price feed information, manipulated by malicious actors. In the shock phase, there would be a situation of malfunctioning of the trading platform, that would cause errors for the entered trades such as the rejections of orders and errors in reporting the actual positions of the investors. Moreover, the investors could observe different data and prices. The amplification phase is caused by the network characteristics, that lead to a rapid expansion of the problem to a large number of market operators, by the uncertainty caused in the market due to the actual situation, and by concurrency of various operators in increasing the financial impact through their reactions to the malfunctioning. This situation could lead to a systemic event if market makers and traders try to exit rapidly from their positions by selling commodities and futures and depressing their prices. After that, a situation of distress both for the providers of the commodities and for the financial institutions that act as intermediaries could occur. The situation of market panic follows a self-sustaining and reinforcing path. Since the accuracy of information is questionable, people cannot rely on the available information and act according to a diffused loss of confidence, and the CCP could incur losses that exceed the minimum default fund required to these kinds of intermediaries. These last passages could lead to a situation of systemic crisis, caused by the liquidity problems of those intermediaries.

³⁴ Ros, G., European Systemic Risk Board, (2020), Occasional Paper Series No 16

In this regard, various studies have analyzed the impact of cyber-attacks on the stock price of the concerned entities. In 2017, Oxford Economics and CGI developed a joint analysis of the impact of cybercrime on listed companies³⁵.

They analyzed 65 companies in all sectors and different countries in the world and their stock performances from 2013 to the first half of 2016. The results indicate that companies which suffered severe data leaks in the period of analysis lost on average **1.8%** of the market capitalization in the week after the disclosure of the event, with respect to the benchmark, composed of companies that weren't affected by cyber incidents.

Another study from the Ponemon Institute and Centrifly study published in May 2017³⁶, analyzed a sample of 133 firms shows how affected companies showed an absolute drop of **5%** in stock value in the period of observation after the disclosure of a data breach. However, the vast majority of the companies in this analysis seems to recover within 45 days from the disclosure of the incident.

In the article published by Eli Amir et al. "*Do firms underreport information on cyber-attacks? Evidence from capital markets*"³⁷ the authors discovered how the impact on the stock prices also depends on the methods of disclosure of cyber-attacks. According to their analysis, firms that decided to disclose directly the news faced a decline of **0.7%** of the stock value, while firms that decided to hide the event incurred higher losses, amounting to **3.7%**. This evidence shows the crucial role that is played by confidence in the financial markets.

Notwithstanding all these studies, according to the article published by Huang and Madnick in the Harvard Business Review, "*a cyberattack doesn't have to sink your stock price*"³⁸ the impact of the disclosure of cyberattacks is still ambiguous.

³⁵ CGI and Oxford Economics, (2017), The cyber value connection

³⁶ Centrifly and Ponemon Institute, (2017), The impact of data breaches on reputation & share value

³⁷ Amir, E., et Al., (2018), Do firms underreport information on cyber-attacks? Evidence from Capital Markets

³⁸ Huang, K., et Al., (2020), A cyberattack doesn't have to sink your Stock Price

This article reports data coming from different studies concerning various important cyber-attacks on listed companies. For example, the hack affecting Capital One that was disclosed in July 2019, and according to an article published by Gunjan Banerji³⁹ made the stock price drop by **6%** during the after-hours trading session, with a low on the day of the disclosure of **7.9%** of the opening price, while it lost the **13.89%** over the two weeks following the cyber disclosure.

Accordingly, also the announcement of the data breach reported by Equifax in September of 2017 had a tremendous impact. The stock of the consumer credit reported a huge drop after it was revealed that the data of 143 million American consumers were put in danger. From the high of September 7th 2017 of **\$143.27** the stock value plunged in the following week, reaching a value of **\$92.98**.

On the other hand, when JP Morgan chase announced a data breach concerning the personal information of 76 million customers⁴⁰, the stock had an immediate response with a slight decrease in the stock price, while during the following year the stock experienced a small growth in value. This event can be seen as proof that the loss of confidence in a financial institution does not depend only on the occurrence of a data breach, but also on the action that a firm takes following the cyber-attack. JP Morgan chase managed to mitigate the impact of reputational damage over its stock price by taking immediate action and increasing its spending on cybersecurity. Moreover, hackers couldn't access financial information but only personal data, making the impact on the confidence over the financial institution milder.

We can sum up by saying that the final impact on a financial institution depends both on the actual measures displayed and on the decisions a company takes to improve its defensive measures. These are two of the main reason that led supervisors and government to define increasing standards of cybersecurity for the financial institutions and to the process of standardization that is occurring in the latest years with the NIS directive in Europe and with the NIST cybersecurity framework. The improvement of the level of cybersecurity of the whole system is thus fundamental for the soundness of the financial

³⁹ Banerji, G., (2019), Capital one Shares Fall Nearly 6% After Breach

⁴⁰ Rushe, D., (2014), Jp Morgan Chase reveals massive data breach affecting 76m households

sector and for the confidence in financial institutions, both necessary to avoid a situation of systemic risk that can lead to a financial crisis

As it is difficult to analyze the cost of a systemic event that hasn't already occurred, some studies have tried to quantify the annual global cost of cybercrime. According to the report published in 2020 by McAfee and CSIS Uncovers⁴¹, global losses stemming from cybercrime during 2020 have exceeded **\$1 trillion**, thus experiencing a **50%** growth from 2018, when the estimated losses amounted to **\$600 billion**. The growing cost is reflected not only in the costs that each company is facing but also in the number of companies affected, since two-thirds of the companies that took part in the survey reported to have been victims of cybercrime during 2019, accordingly increasing the total costs incurred to detect these incidents. The report also states that almost **92%** of the companies affected by a cyber-incident reported monetary losses. As already analyzed in the first chapter, the losses are due to brand and reputation damage, response cost, reduced efficiency of the operation, and increase in spending in cybersecurity. Moreover, the operational losses due to system downtime have to be taken into account.

For what concerns the single countries and also continents, it is important to evaluate the systemic effects that could affect the country/continent system and its economy. These are qualitative aspects, that can be seen as the sum of the single impacts of each event. A safer cyberspace means a safer and even more solid economy. This aspect can lead to the following aspects:

- 1) A progressive loss of competitiveness** of the country's financial institutions and firms for the benefit of those of foreign countries. Safer economies gain and maintain competitive advantages and attract more investors.
- 2) A reduction of the intellectual capital** of the affected firms, that can arise from the loss of profitability due to the loss of consumers.
- 3) Loss of confidence** in the nation's technologies, leading to an increase of dependence on foreign suppliers of essential services with a high level of knowledge. If consolidated through time, this situation can lead to the formation of foreign

⁴¹ CSIS and McAfee, (2020), The hidden cost of cybercrime

monopolies founded on the exclusive ownership of crucial resources, such as technological know.

- 4) Decrease in research and development investments**, followed by a reduction in the quality of employees training and available know-how.
- 5) Increase in unemployment** due to the loss of jobs in the cybersecurity sector and due to the loss of competitiveness of the country/continent economy.

These economic aspects are also followed by a diminishing level of cybersecurity of the country given by the dependence on foreign technological systems. Growing threats are posed by cyberterrorism and cyberespionage, which are malicious activities of hackers backed by governments. Governments gain from the loss of competitiveness of foreign economies and in particular some countries such as Russia and North Korea attempt to disrupt the economic system of western nations to gain economic and political advantages.

This last paragraph has analyzed the economic and systemic consequences that could hit firms and financial institutions. To sum up the possible economic consequences of a cyber incident, situations of financial distress caused by the malfunctioning of financial intermediaries and essential services for the financial sector could lead mainly to three situations⁴²:

- 1) Interbank credit shock**, due to the impossibility of banks, both for operational and liquidity problems caused by a financial attack, to fulfill their payments and settle interbank payments in time. The losses incurred could lead to the default of the lenders and could decrease the confidence in the financial system, spreading the impact not only to the affected institutions but to the financial system as a whole, and due to the high interconnection between banks, losses incurred by a single institution can rapidly cause losses to other financial institutions.
- 2) Market Liquidity Shock**, mainly caused by the losses caused by the decrease in the value of the assets owned by the financial institutions when affected by a financial attack such as a data breach. In this situation the fall in the value of assets can lead the affected institution to fire sale them, further decreasing their value and hurting

⁴² Ros, G., European Systemic Risk Board, (2020), Occasional Paper Series No 16

the balance sheet of the institution. Also in this case, a single cyber incident could lead to a systemic crisis.

3) Funding liquidity Shocks, similar to the market liquidity shock. An institution that is affected by a cyber-incident causing losses and leading to the fire sale of its asset, could be unable to access funding and liquidity by borrowing in the interbank market. In this situation of distress, the fire sale of illiquid assets makes the price of those assets further decrease, affecting all the financial institutions and causing losses for all the banks. Due to this situation of uncertainty, financial institutions cut off their lending activities to keep the liquidity requested by regulations and to fulfill their obligations, causing a situation of credit freeze in the interbank market and for retail customers.

To conclude the economic analysis, we are going to analyze a case study, in order to summarize the impact of a cyber-attack on financial institutions and its implications for the financial environment.

2.2 A PRACTICAL CASE STUDY: COSMOS BANK SWIFT/ATM CYBER-ATTACK

To better understand the impact that an attack on a financial institution could have on the entire financial system we are going to analyze the heist that occurred in August 2018 that affected Cosmos Bank, the 2nd largest cooperative bank in India. Cybercriminals were able to enter the SWIFT system of the bank by launching a sophisticated and strongly coordinated attack on the Indian bank, by using a malware that created a “proxy switching system” able to respond to ATM withdrawal requests. This proxy de facto substituted the regular system owned by the bank and interconnected with the ATM all around the world and allowed **14,000** malicious transactions in **28** countries, among which more than **2000** occurred in the home country of the bank, in less than two hours. We are going to use the model developed by the ESRB to better understand the dynamic of the incident.

Context Phase: On August 11th 2018, cybercriminals were able to enter into the bank’s systems and introduce a malware capable of coordinating transactions by sending fake authorizations through the SWIFT systems to ATMs. The malware approved a large number of fraudulent transactions by using a huge number of cloned debit cards. On the very first day of the attack, cybercriminals were able to send **\$2 million** of fraudulent payments through the transfer of electronic funds to hidden balances. All the traces of these transactions were wiped out.

Shock Phase: At first, the shock was limited to the operational impact. In fact, by introducing the malware and creating a system able to switch payment coordinates that allowed thousands of fraudulent withdrawals through ATMs in India and all over the world, the systems were corrupted. The overall financial losses incurred by Cosmos Bank amounted to **\$ 13.5 million**.

Amplification Phase: Fortunately, even though at first cybercriminals were able to wipe all the traces of their actions, only the databases of Cosmos bank were damaged. Even though the ATM systems are linked to financial institutions from different countries, the malware did not spread to other institutions and only affected the Indian bank. There was no amplification outside the affected institution, thus limiting the negative impact on the confidence toward financial and payment institutions.

Systemic Event phase: The losses incur the bank and the moderate operational impact faced by Cosmos, were not large enough to generate the spillover effect of contagion through the financial system. Since the event did not cause any concern regarding the security and soundness of the payment system, it did not generate a situation of systemic crisis. On the other hand, it was a useful example of the need to increase the level of security and monitoring systems used by financial institutions.

This incident demonstrates how sophisticated the cyber threat has become. Cybercriminals are highly coordinated, work in groups, and sometimes are backed by governments. In this case, the high level of coordination allowed the criminals to operate in 28 different countries and to subtract **\$13.5 million**. Even though cybercriminals were seeking profit, the cyber-attack could have been worse, for example through the acquisition and destruction of sensitive data of the bank customers. Fortunately, no other financial institution was affected and a situation of systemic event was thus prevented. This was also possible to the high level of cybersecurity measures employed by the actors active in the financial system. The criminals managed to transfer the acquired funds to a bank based in Hong Kong, and after that all the traces were wiped out. It is currently unknown how cybercriminals were able to enter into Cosmos Bank's systems. Is possible that they entered the system through phishing, and later on leveraged the system to exploit the vulnerabilities present in the ATM/SWIFT infrastructures. The attack is currently attributed to Lazarus Group⁴³, a state-backed organization based in North Korea.

⁴³ Kolesnikov, O., (2018), Securonix Threat Research Team, Cosmos bank SWIFT/ATM US\$13.5 million cyber attack detection using security analytics

CHAPTER THREE

Governments and Central Banks oversight and regulation

3.1 CYBERSECURITY LAW AND INTERNATIONAL COOPERATION

The definition of the laws and oversight mechanisms used to fight cyber-crime is of fundamental importance to understand how governments and firms deal with this threat. According to Kosseff article in the Iowa Law Review⁴⁴, to form a clear definition of cybersecurity laws, it is important to identify the values that should shape the cybersecurity legal framework by answering some fundamental questions. First of all, it is fundamental to have in mind what we are securing, to define clearly the assets involved. Then we have to define where and who we are securing since a rule involving cyberspace as a whole will be different from a rule defining the security of Interbank Payment systems. Moreover, we have to specify how we intend to protect our assets and when we intend to do so, to give a definite temporal space to our initiatives. Lastly, we have to define the reason why we intend to secure it, to develop rules that are specific to the threat we face. After answering these questions, Kosseff⁴⁵ developed his definition of cybersecurity law:

“Cybersecurity law is the legal framework that provides the confidentiality, integrity, and availability of public and private information, systems and networks, through the use of forward-looking regulation and incentives, with the goal to protecting individual rights and privacy, economic interests and national security”

Accordingly, the implementation of an adequate legal framework is important to guarantee the protection of critical and fundamental assets and infrastructures. Among assets, the information flows have great importance. Cybercriminals exploit information of all kinds, from financial to personal ones, to perpetrate their crimes and to raise money. For these reasons, legislators and politicians have tried and keep on trying to develop effective and efficient rules to limit offensive acts perpetrated in cyberspace.

⁴⁴ Kosseff, J., (2018), Iowa Law Review, Vol.103, No.985, Defining Cybersecurity Law

⁴⁵ Kosseff, J., (2018) Iowa Law Review, Vol.103, No.985, Defining Cybersecurity Law, (p.985)

Even though there are specific rules for different sectors, cybersecurity is a matter of cross regulatory interventions. Normally, these laws rely on the standardization of certified models, which can be applied to evaluate the possible damages of a cyber incident.

Cybersecurity laws base themselves on a mix of cooperation between countries, institutions, and firms, and are displayed on various levels, from the private sector with private firms, to the public one with national and international institutions. Furthermore, the political frameworks of different countries are crucial for the definition of cybersecurity laws and cooperation. Cyber-crime does not affect only single institutions or countries, but has a strong impact on the stability and soundness of the market infrastructures all over the world, due to the high interconnection between them. It is important to improve a legal system that could prevent the spillover effect of an attack through different countries. For these reasons, international organizations such as G7 and the World Economic Forum are approaching this problem with an increasing focus, to give a strong and coordinated response.

For instance, during the 2016 G7, a document called "*G7 Fundamental elements of cybersecurity for the financial sector*"⁴⁶ has been drawn up. In this document, the G7 representatives developed eight non-binding, and high-level fundamental elements tailored to address cyber risk in the financial sector, both for public and private entities. These fundamental elements are intended as the building blocks upon which any institution can design and implement its cybersecurity strategy. Moreover, these elements are deployed to provide an operational strategy to allow a dynamic process to re-evaluate the already existing cybersecurity framework, to be aligned with the latest threats of a continuously changing environment.

⁴⁶ G7 Cyber Experts group (2016), G7 fundamental elements of Cybersecurity for the financial sector

Furthermore, regarding the public authorities, these elements are seen as guidance to develop efficient public policies, regulation, and supervision mechanisms and efforts. To improve the overall cybersecurity and resilience level of the international financial system, firms and public entities have to work together.

The eight elements identified by the cyber experts are the following:

- 1) Cybersecurity strategy and framework.** It is fundamental to establish and maintain a cybersecurity strategy and framework which is specific to the evolving cyber risks and in line with international, national, and industry standards and guidelines, to reduce cyber risk with an integrated effort.
- 2) Governance.** The definition of roles and responsibilities for the implementation of a cybersecurity strategy is fundamental to manage and oversee efficiently the cybersecurity strategy. This mechanism reinforces accountability and fosters communication among different operating units, firms, and institutions.
- 3) Risk and control assessment.** Entities must evaluate cyber risks as a part of overall enterprise risk. To do so, it is important to identify and assess effective control mechanisms like systems, policies, and cybersecurity procedures and training.
- 4) Monitoring.** The establishment of standardized monitoring processes to detect possible cyber threats and evaluate the effectiveness of controls. This process includes exercises to test the level of cybersecurity of an institution.
- 5) Response.** Firms and institutions have to set up an efficient response mechanism, that to be effective it has to timely assess the nature of the attack, its extent, and its impact. Then it has to limit the damages caused by the cyber incidents and attenuate the impact on the firm. The entity attacked has to notify the cyber incident to stakeholders such as authorities, shareholders, and third parties that could be damaged by the attack such as services suppliers, and eventually coordinate the needed response activities.

- 6) Recovery.** To fully recover, firms have to resume their operations responsibly, by learning from the cyber incidents. They have to identify and eliminate all the vulnerabilities that could lead to similar situations, then they have to restore the systems and data to a normal state. It is fundamental to assure operational stability and firm integrity to allow the critical economic function of all financial intermediaries and to avoid possible repercussions on the economic system.
- 7) Information sharing.** Information sharing is of vital importance. Firms have to engage in the timely sharing of reliable information about cyber incidents. The information-sharing process increases firms' and institutions' awareness, allowing them to adapt their active security framework to new threats. This information sharing flow between entities and public authorities enhances the disposable know-how and increases the overall cybersecurity level.
- 8) Continuous learning.** The objective of all the previous elements aims at ensuring a process of continuous learning for firms and institutions. The cooperation between the public and the private sector allows for a proactive process of revision and adaptation of the current framework, which is needed to effectively face threats that are always evolving.

The G-7 published the "*Fundamental elements for effective assessment of cybersecurity in the financial sector*⁴⁷", to promote the effective practices outlined in the G7 Fundamental elements of cybersecurity for the financial sector. This document focuses on how to perform and assess the practices outlined in the previous paper. It does so by describing a set of desirable outcomes that each entity should exhibit or at least aim at developing, and a set of assessment components, that can be used to develop a framework to quantify the progress achieved in building and enhancing a cybersecurity strategy.

⁴⁷ G7 Information center, University of Toronto, (2016), G7 Fundamental elements for effective assessment of cybersecurity in the financial sector

Table 2: G7 Fundamental elements for effective assessment

DESIRABLE OUTCOMES	ASSESSMENT COMPONENTS
<ol style="list-style-type: none"> 1) Firms follow the eight Fundamental elements. 2) Cybersecurity influences decisions making process 3) Cyber incidents are taken into account. 4) The approach to cybersecurity is adaptive and changes over time. 5) Cybersecurity is driven by informed and secure behaviors of institutions' components. 	<ol style="list-style-type: none"> 1) Clear assessment objectives are established. 2) Methodology and expectations are clear. 3) Several cybersecurity tools to face a changing threat. 4) Report cyber incidents and remedial actions. 5) Ensure a fair and reliable assessment, based on standardized and certified processes.

Source: <http://www.g7.utoronto.ca/>

G7 fundamental elements for effective assessment of cybersecurity in the financial sector.

Own representation

To underline the importance of the protection of the global financial system against cybercrime, the World Economic Forum and the Carnegie Endowment for International Peace released a paper, "*International strategy to better protect the Financial System Against Cyber Threats*"⁴⁸. This report underlines the importance of collaboration to reduce fragmentation of information flows concerning cybercrime.

⁴⁸ Maurer, T., Nelson, A., (2020), Carnegie Endowment for International Peace, International Strategy to Better Protect the Financial System Against Cyber Threats

In this regard, international cooperation among government agencies, financial firms, and technology companies offering services to these institutions is crucial to guarantee the smooth functioning of the financial system as a whole.

Moreover, another relevant institution such as the **Financial Stability Board**⁴⁹ has addressed the problem of cybersecurity in the financial sector and its implications for financial stability. The FSB underlines the importance of an efficient and effective response to cyber incidents, that has to be followed by an adequate plan to recover from operational and financial distress. It divides the cyber incident in three phases, presenting some guidelines to encourage the use of a cyber incident and response toolkit:

- 1) Before:** Before the occurrence of a cyber incident, financial intermediaries need to engage in the coordination of cybersecurity plans and communication. They must plan and prepare for a possible attack by improving the available cybersecurity measures.

- 2) During:** During the cyber-attack, firms must first focus on the restoration of the operational activities and guarantee an effective recovery of the financial functions. In this phase, it is important to employ all the possible measures to mitigate the possible consequences and analyze the cyber-incident to understand the vulnerabilities that allowed the breach and improve their cybersecurity measures. It is fundamental to keep the authorities informed, to prevent a systemic evolution of the cyber incident.

- 3) After:** After the cyber incident firms must focus only on the improvement of the available measures to prevent new cyber incidents in the future.

This toolkit aims at giving a set of rules to follow in order to prevent the spread of cyber-incidents across the financial sector.

⁴⁹ Financial Stability Board, Cyber Resilience

Source: <https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/cyber-resilience/>

All these documents have in common the importance of information sharing and cooperation to increase the cyber-resilience of the financial sector, and the development of a standardized supervision framework to strengthen the level of cybersecurity. Moreover, it is suggested the creation of **CERTs**, Computer Emergency Response Teams, which are national bodies specialized in handling cyber incidents for critical assets. These bodies play a crucial role in the improvement of national and international cybersecurity and try to protect critical assets and infrastructures of interest, such as financial firms and telecommunications.

Collaboration among countries, with some exceptions, is increasing since governments recognize the importance of the smooth functioning of critical infrastructures all over the world. As further analyzed in this chapter, institutions are adopting laws and regulations to increase the exchange of information between firms and institutions and between institutions of different countries. Even though the protection of critical assets and economic interests between competing countries remains crucial, the exchange of information benefits all the actors, enhancing the response capacity to new cyber threats.

3.2 THE US CYBERSECURITY LEGAL FRAMEWORK

In the United States of America, the legal framework is more fragmented than in the EU. The US government is organized as a Federal presidential constitutional republic, so it will present both federal laws applying to all states and local laws applying to single states.

The **NIST Cybersecurity framework**⁵⁰, published by the US National Institute of Standards and technology in 2014, is considered the US equivalent of the NIS directive. This framework establishes a set of voluntary standards and best practices for every industry to prepare firms and institutions to identify and better assess cyber risks. The fact that these guidelines are not mandatory may limit the positive impact of the NIST framework on different industries. In 2020 the percentage of firms following this framework was around 30%, including some important firms such as Amazon and JP Morgan Chase⁵¹.

The NIST framework set different goals:

- 1) Coordinates industries-specific standards with the best practices offered by the guidelines to help firms to administer cybersecurity problems properly.
- 2) It wants to provide a common and diffused framework to allow workers to develop a widespread culture about cyber risk and cybersecurity.
- 3) It grants guidelines and strategies on how to avoid risks and on how to reduce them.
- 4) Offers advice on how to react to cyberattacks and how to resume business continuity.

To reach its goals, five critical areas are covered, which will be the fundamental areas for an efficient cybersecurity strategy.

⁵⁰ Source: <https://www.nist.gov/cyberframework/perspectives>

⁵¹ Hall, J., (2020), A guide to the NIST Cybersecurity Framework
Source: <https://www.ifsecglobal.com>

The five areas of intervention are the following:

- 1) Identification:** It is important to identify risks by looking at current and past data to understand and identify cyber threats. An analytical approach to risk analysis is required, as cyber risk has to be treated like any other risk the company faces.
- 2) Protection:** Understand the elements facilitating an efficient protection strategy. Some elements in this area are more important than others. For example, an effective data protection mechanism plays a crucial role.
- 3) Detection:** Companies offering strongly interconnected services as the financial ones have to be ready to recognize cyberattacks. Promptly assessing a cyber incident may reduce its repercussions on the whole financial system.
- 4) Response:** An efficient response mechanism is decisive to reduce the impact of cyberattacks.
- 5) Recover:** Companies have to set plans explaining the necessary steps to recover from cyber incidents effectively.

The framework offers also a mechanism to assess the level of cybersecurity reached according to measures applied by firms. The different levels of cybersecurity are divided into tiers, from tier 1 to tier 4. Tier one means that the firm has applied partially the measures needed to adequately face the cyber risks already experienced. Tier two firms are risk-informed companies, namely companies aware of the risks they are facing and that are planning on how to face them. Tier three firms are organizations that have set clear cybersecurity processes that can be easily repeated by the firm in case of need. The higher level is represented by tier four, firms that can adapt their cybersecurity strategy to different threats. These firms proactively integrate their cybersecurity framework to be able to face attacks of different nature.

This framework has been revised in 2018, to adapt it to current threats. The evolving nature of cybercrime makes it paramount the process of revision of outdated laws. In this sense, the NIST framework was implemented with the establishment of the Cybersecurity and Infrastructures Agency, **CISA**, which has the same role as the ENISA agency in Europe.

It is important to underline that the US does not have a diffused and comprehensive law concerning Data privacy. There is no equivalent law such as the European GDPR, standardizing the approach to data privacy for all states. In the US each state decides on its guidelines on data privacy. To fill this gap, in 2020 Senator Kirsten Gillibrand proposed the institution of the Federal Data Protection Agency, to act at a federal level with enforcement powers comparable to the competent institutions in Europe⁵².

The **Gramm-Leach-Bliley Act**⁵³, known as the Financial Services Modernization Act, was enacted in 1999. It protects the privacy and security of personal financial information of consumers, by requiring financial intermediaries and firms to follow certain privacy standards and to adopt adequate security standards to protect personal data. Moreover, firms must explain precisely how they manage the information-sharing process and consumers have the right to decide if they do not want the firm to share their personal financial information and data with other institutions. To respect the security standards, financial firms must ensure the protection of confidential customer records from both unauthorized and fraudulent access that could cause damages, and from cyberattacks. Besides, the GLBA enabled several federal agencies such as the SEC, the Federal Trade Commission, and the Consumer Financial Protection Bureau to enact complementary regulations to ensure adequate privacy and security levels for financial institutions.

For instance, California hosts the majority of fintech companies in Silicon Valley, which manage every day an outstanding amount of private data. For this reason, the state of California has developed several laws concerning this issue.

⁵² Ikeda, S., (2020), New legislation in the U.S Proposes Federal Data Protection Agency, Broad Range of new Enforcement Actions

Source: <https://www.cpomagazine.com/>

⁵³ United States Congress, (1999), Gramm-Leach-Bliley Act

California cybersecurity law provides for a general set of cybersecurity rules, also on how to notify data breaches. Business and IT providers must apply adequate processes and practices for the protection of data from unauthorized access, illegal use, destruction, and disclosure. If a business has a contract with other entities, also the counterparts of the contract must apply the guidelines imposed by California's rules. California law obliges businesses to grant written notice of breach occurrence to the national authority, to any person and related business involved. Financial institutions have specific and stricter requirements, specified in **the California Financial Information Privacy Act**. It was enacted in 2003 and asks financial firms "to *provide their consumers' notice and meaningful choice about how consumers' nonpublic personal information is shared or sold by their financial institutions*"⁵⁴. This act aims to grant people a greater level of privacy and data protection than the one granted by the Gramm-Leach-Bliley Act.

The state of New York has stricter requirements concerning cybersecurity issues, due to the importance of cybersecurity for the city of New York, which is considered the first financial center of the world according to the Global Financial Centers Index⁵⁵. **The New York Department of Financial Services** monitors closely the growing risks posed by cybercriminals to financial systems. The growing threat obliges firms to test their systems periodically to detect possible vulnerabilities to avoid relevant financial losses. The burden on financial firms is heavier in a center such as New York City for the higher risk of spillover effect. The protection of financial assets, such as data and information, needs to be a priority for all the actors of the financial industry.

Accordingly, the **NYFDS Cybersecurity Regulation**⁵⁶ was enacted in 2017 and applies to different companies, such as state-chartered commercial and investment banks, foreign financial institutions operating in the city, insurance companies, and all those companies providing services to them.

⁵⁴ California Financial Code, (2003), California Financial Information Privacy Act

Source: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=1.4.&lawCode=FIN

⁵⁵ Source: <https://www.longfinance.net/programmes/financial-centre-futures/global-financial-centres-index/gfci-29-explore-data/gfci-29-rank/>

⁵⁶ Cybersecurity requirements for Financial Services Companies

Source: <https://govt.westlaw.com>

The strict rules imposed range from the implementation of a detailed cybersecurity strategy to the designation of a competent officer, the **Chief Information Security Officer**, also called CISO, that has to control the compliance of the firm's strategy with the rules. To comply with the NYDFS Cybersecurity Regulation, a cybersecurity program needs to adopt all the guidelines listed in the NIST Cybersecurity Framework and **the ISO 27001 Standards**⁵⁷, a set of specific requirements for the management of the security of information systems. Data Breaches need to be notified within 72 hours from detection, and the CISOs have to prepare an annual report including information about the firm's cybersecurity policies and procedures, the risks and threats faced in its business activity, and the efficiency of the organization's current measures. Moreover, the level of cybersecurity has to be continuously analyzed, to respond proactively to new threats. The compliance with existing rules needs to be certified annually by companies' CISOs.

Financial Markets are under the supervision of the **Securities and Exchange Commission**. The SEC is responsible also for the aspects of cybersecurity, even though cybersecurity is considered a responsibility of all the participants in the market. Moreover, it collaborates with government agencies such as the FBI, the CISA, and the US government itself to ensure the respect of the enacted rules⁵⁸.

As it happens in Europe with the ECB, the US central bank, the **Federal Reserve**, aims at ensuring the operational resilience and continuity of financial markets intermediaries and infrastructures. These aspects are essential to ensure trust in the financial industry, to avoid bank runs that could lead to a deeper financial crisis. As a result of the higher reliance on technologies of the financial industry, the capability to restore the operativity of financial intermediaries has become more important over the years. The Federal Reserve is aware of the interconnection of the banking and financial sector throughout the world, and hence collaborates with the ECB and with the UK Prudential Regulatory Authority to ensure cooperation and coordination concerning the supervisory approach on operational resilience.

⁵⁷ Source: <https://www.iso27001security.com/html/27001.html>

⁵⁸ Source: <https://www.sec.gov/spotlight/cybersecurity>

The increased sophistication of cyber threats and the growing reliance on external providers of services endure the exposure of firms to various operational risks. The most important aspect covered by the FED in its guidelines is operational resilience, which is defined as "*the ability to deliver operations, including critical operations and core business lines, through disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.*"⁵⁹

Hazards and human errors may not be prevented, even if an appropriate level of expertise may certainly limit them, but an adequate operational resilience approach may enhance the capacity of financial intermediaries to adapt and prepare the organizations to recover from damages caused by cyber incidents.

⁵⁹ Federal Reserve, (2020), Supervisory policy and Guidance Topics

Source: <https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm>

3.3 THE EUROPEAN LEGAL FRAMEWORK AND THE EUROPEAN CENTRAL BANK

The European legal framework follows the international guidelines expressed by the G7 and by other international organizations. The European Union developed both specific and cross-sectorial legislation concerning cybersecurity. In this paragraph, we are going to analyze the most important pieces of legislation that have been enacted by the European Parliament, such as the European NIS directive, the Cybersecurity Act and the GDPR, and the strategy upon which the European Union, through the ECB and its specific bodies aim at protecting its financial markets and critical infrastructures.

The process of creation of cybersecurity laws has occurred mainly in the last decade. Before this period, there were only some legislations that made the digital environment safer, which were not too specific. The first regulation regarding cybersecurity was the **1995/46/EC**⁶⁰, which is focused on the processing of personal data. After that, another important point for a coordinated response to cybercrime was met in 2001, when during the convention of Budapest, the Council of Europe set the first specific provisions to fight cybercrime.

The first act towards the harmonization of the cybersecurity strategy is the decision to build a common and consolidated European Digital Single Market. From 2013, with the final version of the **Join/2013/01**⁶¹ communication to the European parliament. Since cyberspace is vast and highly connected, cyber threats have to be faced by the European countries as a common problem to make the single market work well. To reach this goal, the European Union decided to build an integrated European digital single market, a five-year plan for digital and cybersecurity development.

⁶⁰ European parliament and council, (1995), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals about the processing of personal data and the free movement of such data

⁶¹ European Commission, (2013), Joint Communication to the European Parliament, the Council, the European Economic Committee, and the Committee of the region

Through this act, cybersecurity becomes a strategic matter in European policy. From this point onward, a substantial effort from all the member states is required to reach the goals set by the strategy.

The first goal is the achievement of an adequate level of **cyber resilience**, which is the ability of entities to continuously deliver their services despite the occurrence of adverse cyber incidents. The second goal set is the promotion of **cyber deterrence**, which is the use of credible and dissuasive measures to discourage any potential cybercriminal.

Then we have three guidelines that must be followed by public and private institutions to allow for a correct application of the cybersecurity strategy. The creation of a **cyber-defense policy**, the development of industrial and technological resources for cybersecurity, to avoid a heavy reliance on foreign companies, and the establishment of a **coherent international cyberspace** for the EU, to promote the EU core values, such as inclusion and integration.

To protect data, one of the crucial assets found in cyberspace, the European Union enacted a specific regulation. The General Data Protection Regulation, also known as **GDPR**⁶² (Regulation 2016/679) is the most important legislation regarding the protection of consumers' data. It repeals the previous directive 95/46 of the European Commission. In this regulation, is introduced a risk-based approach adopted by the European Union. The introduction of the concept of direct accountability of security managers enhances the level of attention given by public and private institutions to the management of personal data. Moreover, another important theme involves the importance of information sharing regarding data breaches. Lastly, the concept of security by design and by default is introduced, directing public and private institutions to possess the technical and security characteristic needed to manage data from the acquisition, not only after the occurrence of a cyberattack. Moreover, with the GDPR the figure of the **Data Protection Officer** was introduced. The DPO is a specialist that has the role of informing the competent authorities of Data breaches, oversees the company's procedures regarding data and privacy management, and adapts current companies' procedures to the latest regulations. The main goal is to ensure compliance with GDPR guidelines.

⁶² European Parliament and Council, (2016), Regulation (EU) 2016/679 of the European Parliament and the Council

The first piece of EU cross-sectoral legislation on cybersecurity is the Directive on Security of network and information systems, also known as **NIS DIRECTIVE (EU DIRECTIVE 2016/1148)**⁶³. This directive was initially released on the 6th of July 2016 and provides a legal framework to increase the level and the quality of cybersecurity in EU countries. This common legal framework has to be adopted by the member states and concerns information system security and the obligation to notify, to increase the level of cooperation among EU countries.

Great importance is given to the control measures used to guarantee a high cybersecurity level to **OES**, Operators of Essential Services, defined in the fifth article of the NIS directive. OES are public and private institutions, performing essential services for society and the economy in different sectors, like banking and financial markets. They have stricter requirements in terms of security measures, and notification obligations of serious incidents. Then other actors playing an important role are **DSPs**, Digital Services Providers, that are the legal persons performing a digital service, which according to the **EU DIRECTIVE 2015/1535**⁶⁴ is a service provided normally by electronic means and for remuneration, needed by the recipient to carry out its activity.

After defining the actors having a strong impact on the cybersecurity of the European countries, the NIS directive defines provides for the definition of:

- 1) A network of interconnected intervention groups for information security in case of cyber incidents, known as **CSIRT**, Computer Security Incident Response Team, to ensure coordinated and unitary management of cyber incidents at a national level and the competent national NIS authority. In order to have prepared member states, it is necessary to ensure an appropriate organization and equipment.

⁶³ Source: <https://digital-strategy.ec.europa.eu/en/policies/nis-directive>

⁶⁴ European Parliament and Council, (2015), Directive (EU) 2015/1535 of the European Parliament and Council

- 2) A unique NIS focal point, to ensure the coordination of security issues at a national level and the necessary connection to guarantee cooperation and information exchange between the Italian competent authorities with those of the other European countries. At a European level, Cooperation is ensured by the NIS Cooperation Group, **NISCG**, which aims at supporting the process of cybersecurity standardization.

- 3) A diffused cybersecurity culture to increase Member States' awareness about cybersecurity across the essential sectors of the economy. This point is particularly important for those sectors that necessarily rely on the use of Information Technologies to carry out their core activities, such as banking, financial markets, and digital infrastructures. Nevertheless, the NIS directive gives Member states the possibility to extend the scope of application of the directive to sectors not considered essential by the NIS.

As we have seen, the NIS directive comprehends both coercion, such as the obligation to notify and to follow stricter rules for the OES, and arbitrary decisions, such as the possibility to comprehend sectors different from the one included in the NIS directive in national pieces of cybersecurity legislation. To guarantee the satisfaction of legal requirements by OES and DSPs, every cyber incident that could harm the continuity of an Essential Service has to be notified to the competent national authority and the CSIRT.

This obligation also applies to Digital Services Providers upon which essential services rely on. Notifications of incidents need to be submitted within 72 hours after discovering the cyberattack. After that, the CSIRT has to decide whether to inform the public or not about the cyberattack. When the information is considered fundamental to prevent similar incidents, OES and DSPs are informed about the risk. To determine if the impact of the cyberattack is substantial different parameters are taken into account: The number of interested users, the duration of the cyber incident since if a cyber incident is instantly detected the impact and the amount of data acquired by cybercriminals will be lower, the geographic diffusion of the interested area, the impact on the functioning of the service providers and the possible scope on social and economic activities.

Notwithstanding all those rules, European institutions are aware that the creation of national authorities managing cybersecurity issues is vital, for two main reasons: Private companies are unlikely to take the negative impact of their actions on their network into account, and since many of those companies collaborate with national institutions to deliver critical services, their level of cybersecurity is of crucial importance to guarantee a safer financial environment. So, the risk of under investments in cybersecurity has to be taken into account and managed carefully. The second concern is the reputational risk linked to information-sharing since firms might tend to hide vulnerabilities and cyber incidents information to the competent authorities to avoid reputational costs.

To ensure the respect of the NIS directive, member states established rules about sanctions in case of violation of national provisions. These provided sanctions are effective, proportionate to the damage caused, and dissuasive. Member states have notified these norms to the European Commission on the 9th May 2018.

The European Commission has started a public revision process on the 25th of June 2020⁶⁵, considered the changing technological scenario in the latest years and the implications deriving from the current COVID-19 pandemic. This process opened to all stakeholders in the essential sectors and the institutions of the European countries aims at analyzing the level of functioning of the NIS directive for the members of the EU. This new proposal, called **NIS2**, aims at evaluating the benefit to cost ratio, derived from the revision process of the NIS rule.

As a result of the EU commission revision process, it was found that most of the EU states weren't able to apply efficiently the initial version of the Directive, with some differences between states, going against the standardized and harmonized model of the directive. However, the fragmentation characterizing the ICT world harms a correct application of the NIS directive.

⁶⁵ Tosoni, L., (2020) Verso una direttiva NIS 2, che cambia le proposte della commissione UE
Source: <https://www.cybersecurity360.it/legal/>

The remarks presented in the revision process are based on the concept of amplification of the scope of the directive through an approach of *security by design*⁶⁶:

"Security by design means that companies think about cybersecurity at the beginning of a project. Secure by design means that software engineers have designed the software to be secure from the outset to reduce the likelihood of flaws that might compromise a company's information security"

In this regard, growing importance is given to the concept of prevention. The NIS2 will probably present an extension of the specific cybersecurity duties to other sectors that were previously left out of the directive. Moreover, the criteria to define OESs will be included in the NIS2, and not left to the single states, to increase the uniformity of these categories.

Notification requirements will be stricter in terms of time, with the obligation to notify the incident in the 24 hours following the detection, and fines for member states and firms that do not comply with the directive will be higher, with a maximum of **10 million euros** or up to the **2%** of the annual revenues of the firm. Even though these principles have been set, to see the application by member states will still take some time, due to the bureaucratic process of approval and national transposition.

The NIS cooperation group and the **ENISA**, the European Network of information and security agency, play an important role in this revision process.

The EU regulation 2019/881, on ENISA and information and communications technology cybersecurity certification, also known as the **Cybersecurity Act**,⁶⁷ concerns the revision of the role of ENISA with the repeal of the EU regulation 2013/526. It was enacted by the European parliament on 7/04/2019 and it is considered a fundamental turning point in the European cybersecurity strategy. It aims at promoting the cyber defense of EU institutions and it is considered with the NIS directive the backbone of the EU cybersecurity legal framework.

⁶⁶ Reciprocity Labs, (2020), What is security by design?

Source: <https://reciprocitylabs.com/resources/what-is-security-by-design/>

⁶⁷ European Parliament and Council, (2019), Regulation (EU) 2019/881 of the European Parliament and the Council

This regulation, by posing itself in complementarity with the NIS directive, aims at pursuing some fundamental objectives:

- 1) The reinforcement of the resilience and resistance of the EU to cyber attack
- 2) The creation of a unique market for cybersecurity products, services, and processes
- 3) The increase in trust of consumer and institutions in the use of digital technologies

To reach its goals, a fundamental point is the reinforcement of the ENISA. In the Cybersecurity Act, the ENISA is given a permanent mandate and broader scope. This institution was previously given only consulting tasks, and with the reform, it acquires a role of support to operational management of cyber incidents occurring in member states. The second part of the Cybersecurity Act defines the settings of an institutional framework to allow for the creation of a common certification scheme for digital products and services.

Now we are going to analyze some specific regulations concerning the banking sector and the role of the European banking authority and the ECB. An important act is the EU Directive on payment services in the internal market, the (EU) 2015/2366, also known as **PSD2**⁶⁸. It entered into force on January 13th, 2016, aiming at promoting the development of a more efficient and safer retail payments market. It does so by encouraging innovation of payment systems and improving the level of security of electronic payments. Great importance is given to users' protection. Strict rules about payment institutions are introduced, such as a minimum capital requirement to hold at the time of authorization as a payment institution from the EBA, ranging from **€20 000** to **€125 000**, according to the services the financial institution intends to perform. Moreover, payment institutions must retain a minimum level of own funds also after the recognition, as the minimum capital requirements vary with the volume of transactions and payments passing through the institution.

⁶⁸ European parliament and council, (2015), Directive (EU) 2015/2366 of the European Parliament and the Council

The member states or competent authorities could also require a payment institution to safeguard the funds received from the payment service users for the execution of the transaction. After the registration of the payment providers, the authorization can be withdrawn by the competent authorities if the payment service provider does not respect the rules imposed by the PSD2 directive. Prudential Supervision is granted by the designated competent authority, that has to control that the institutions comply with all its duty.

The **European Banking Authority** has contributed to the creation of a framework to guarantee an adequate level of cybersecurity, by setting out how financial institutions should manage the ICT and security risks that could harm the financial industry. The guidelines provided by the EBA, give detailed insight on how to comply with the **2006/48/EC directive on Capital requirements**⁶⁹ and with the **PSD2**. In particular, article 95 of the PSD2, provides explicit provisions for the management of operation and security risk. Appropriate mitigation measures are required and the EBA has the mandate to develop appropriate guidelines on this subject. Moreover, the EBA published a Roadmap on Fintech⁷⁰ to describe the priorities to follow in order to contain and monitor new cyber threats and analyze the impact on private's business models. The monitoring process and the promotion of best supervisory practices are the fundamental points arising from the EBA roadmap.

The European Central Bank set its strategy to follow the guidelines of the various legislative acts analyzed, both at a European and at an international level. In 2017, the **Eurosystem cyber resilience strategy For FMIs**⁷¹ was approved by the governing council, to improve the cyber resilience of the European financial industry. It does so by improving the readiness with which individual FMIs can react to cyber incidents.

⁶⁹ European Parliament and Council, (2006), Directive 2006/48/EC of the European Parliament and the Council

⁷⁰ Source: <https://www.eba.europa.eu/eba-publishes-its-roadmap-on-fintech>

⁷¹ Source: <https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html>

The focus is on those institutions directly under the supervision of the euro-system central banks. Moreover, this strategy aims at fostering collaboration among FMIs, their fundamental services suppliers, and institutions. This strategy is based on the **CPMI-IOSCO**⁷² guidance and is divided into three pillars.

The **first pillar** is the FMI readiness and aims at ensuring the correct use of the CPMI-IOSCO guidance by encouraging a collaborative approach in the assessment of the security of payment systems in the euro area. Tools such as the European Red team testing framework have been developed by the euro-system and are currently under study to prepare the financial players and test their ability to react to cyberattacks. Cyber surveys are another important tool used by overseers to assess the level of cyber preparedness and promptness of financial institutions.

The **second pillar** concerns sector resilience. The only effective way to fight and face cybercrime is to think of the financial ecosystem as a whole. The high interconnection of financial intermediaries, the level of cybersecurity of other institutions can also impact other financial firms. The level of cyber resilience has to be high enough across the European financial industry, to avoid the spread of offensive acts. Thus, pillar two focuses on increasing the level of cyber resilience of the financial sector by facilitating cross-national and cross-authority collaboration. The establishment of an efficient model of information sharing will increase the level of business continuity and decrease the possible impact of cyberattacks.

The **third pillar** deals with the strategic regulator-industry engagement. Collaboration among institutional and private participants is crucial to ensure a productive defense against cybercrime. Pillar three aims to build trust between all the participants active in the market to ensure regular meetings with participants both from representatives of institutions and from FMIs. For this reason, a specific body to organize and control such meetings was created, the Euro Cyber Resilience Board for Pan-European Financial infrastructures.

⁷² CPMI-IOSCO, (2012), Principles for financial market infrastructures

Cybersecurity is seen as a priority both from the ECB and the European Commission and Parliament, and for this reason, specific investment plans have been developed to ensure the right amount of funds to improve the EU's cybersecurity infrastructures. For example, the **Digital Europe Program**⁷³ plans to invest **€1.9 billion** into cybersecurity for the period 2021-2027. Moreover, the **Recovery Plan for Europe** provides specific provisions for investment in Digitalization, which includes also the strengthening of cybersecurity.

As analyzed in the two previous paragraphs, there are several differences and similarities among the European and the American legal framework. First of all, the European legal framework is more centralized than the US one, since all the different pieces of legislation enacted by different countries are based on the NIS directive. European countries are obliged to adopt the guidelines provided by the directive to avoid sanctions. On the other hand, the US NIST framework is a set of voluntary guidelines, to guide institutions in setting their cybersecurity measures. Another important difference is the absence of a diffused and comprehensive law concerning data privacy in the US, so there isn't a standard approach as the one provided to European countries by the GDPR. In the US each state has its own regulation about this issue, which are stricter in those states where firms manage a higher amount of data such as the state of New York and California. A commonality between these two different frameworks is given by the fact that each of them follows international guidelines as the ISO 27001 Standards, and the various objectives explicitly stated by the various international organizations, such as the G7 and the World Economic Forum. The presence of a group of experts such as the various CSIRT teams is provided by the European and the American frameworks, providing a similar response mechanism to cyber incidents. So, the main difference concerns the possibility of US firms to adopt state-specific rules and different regulations concerning data privacy, based on the own nature of the firms, and the greater central role played by the European Union to harmonize the legal framework for all the European countries.

⁷³ Source: <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>

3.4 ITALY: THE NATIONAL LEGAL FRAMEWORK AND THE NATIONAL CYBERSECURITY PERIMETER

The Italian cybersecurity legal framework follows the directives and regulations enacted by the European Union. The first rule designing a cybersecurity legal framework is the **Decree -Law 179/2012**⁷⁴, which was later converted into law. In this rule it is provided the need to safeguard the national technological autonomy and set the cyber resilience and operational continuity of digital systems and services. In this regard, it was designated the Prime Minister's Office as the central institution to promote and control the development of an adequate level of cybersecurity for national critical infrastructures.

The first specific act concerning cybersecurity is a Decree of the Prime Minister enacted on the 24th of January 2013⁷⁵, also called "**Decreto Monti**", which provides the first definition of the National Cybersecurity Architecture and Critical Infrastructures Protection, designing an organic system under the directives of the Prime Minister itself, that coordinates all the instances of private and public subject of interest.

This decree is followed by the enactment of another important act for the constitution of a comprehensive legal framework, such as the DPCM enacted on the 27th January 2014, adopting the "**Quadro Strategico Nazionale**"⁷⁶ for the national cybersecurity, a framework identifying the profiles and evolutionary trends of cyber threats of the information systems of national interest. Moreover, it defines the roles and tasks of private and public actors, and the procedures to enhance the level of cybersecurity to prepare for future challenges posed by cyber threats.

From the QSN descends another DPCM enacted on the 27th of January 2014, the **PNPC**, the National Plan for Cyber Protection, that indicates the operational directives to implement concretely the guidelines listed in the previous decree.

⁷⁴ Decreto Legge 179/2012, (2012), Ulteriori misure urgenti per la crescita del Paese

⁷⁵ Decreto del Presidente del Consiglio dei ministri, (2013), Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale

⁷⁶ Decreto del Presidente del Consiglio dei Ministri, (2014), Strategia nazionale per la sicurezza cibernetica

To realize the activities of implementation of cybersecurity, the **Cybersecurity Law 208/2015**⁷⁷ allocates for the first time specific funding for cybersecurity, amounting to **€150 Million**, to improve the level of cybersecurity of the public administration.

With the shift of daily activities in cyberspace, the focus on cybersecurity has increased over time, to create competitive advantages and opportunities deriving from a safe cyber environment, both from private and public institutions. For this reason, in 2017 with the **DPCM CYBER**⁷⁸, Prime Minister Gentiloni tried to redefine the national architecture designed in Mario Monti's decree, by assigning a central role to the Department for Information and national securities, the DIS, that becomes the operational institution for the prime minister and the ministers belonging to the inter-ministerial committee for the security of the republic, both for the private sector and public administration. In this regard, it is of central importance the role of the **NSC**, an inter-governmental board with the duty to manage cybersecurity crises and to connect different institutions of the national institutional architecture.

In close connection with the directives enacted by the European Union, Italy and all the member states are required to identify the Essential Services Operators and Digital Derives Providers, from which depends the functioning of the society and the national economy, such as the institutions operating in the financial sector. In the **legislative decree 65/2018**⁷⁹, implementing the NIS directive, it is constituted the Italian **CSIRT**, the computer security incident response team, that performs technical tasks in the prevention and response to cyber incidents in cooperation with the European countries CSIRT.

⁷⁷ Legge di stabilità 2016, (2015), Disposizione del bilancio annuale e pluriennale dello stato

⁷⁸ Decreto del Presidente del Consiglio dei Ministri, (2017), Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale

⁷⁹ Decreto Legislativo 65/2018, (2018), Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

The institution of a national plan of cybersecurity, aimed at ensuring a high level of security of information and computer systems of the public administration and of national public and private operators, induced to the issuing of the most recent directive of the sector, the **Law Decree 105/2019**⁸⁰, converted from the **Law 133/2019** also known as **National Cybersecurity Perimeter**, regulating special powers for national strategic sectors. In this law are set guidelines to determine the actors to be included in this perimeter, and in particular for the financial institutions private banks are included only for the protection of bank accounts and ATMs. In this regard specific rules for financial markets and investment banks are not present. This rule also includes specific provisions for the activities of Mergers and Acquisitions, giving the government-specific powers for national strategic companies, with particular attention to the sectors with high technological development.

Currently, the new regulatory framework of the Perimeter of National Security is incomplete, since to implement all the rules contained in this regulation, indicates the necessity to draft a set of implementing decrees. Only one of these decrees has been enacted, the **DPCM 131/2020**⁸¹, which specifies the categories addressed from the new obligations defined by the National Cybersecurity Plan. Moreover, the **CONSOB** and the **Bank of Italy** developed a common cybersecurity strategy for the security of the financial sector in order to protect financial infrastructures⁸². This strategy aims at reinforcing the current level of cybersecurity, due to the recognized value of a cooperative approach, and regards three intervention areas: regulation and supervision, cooperation between the public and private sector, and development of a diffused knowledge base of cyber threats between financial operators. These institutions use instruments and risk evaluation frameworks offered and already adopted in the euro system.

⁸⁰ Decreto Legge 105/2019, (2019), Disposizioni in materia di perimetro di sicurezza nazionale cibernetica

⁸¹ Decreto del Presidente del Consiglio dei Ministri, (2020), Regolamento in materia di perimetro cibernetico nazionale

⁸² Source: https://www.consob.it/documents/46180/46181/comunicato_cnsb_bi_20200116.pdf/a32d82bf-3e30-42f3-9a91-6c7ccfeeb2ed

CONCLUSIONS

The bond between the financial sector and information technologies is tightening year by year. As new technologies are developed, new applications for the financial sector are introduced, to facilitate the activities of a large number of actors in the industry. But the increased use of technologies poses both advantages and problems to a sector that heavily relies on the security of its operations and of customer information. The evidence presented in the first chapter shows a stable increase both in the frequency and in the severity of cyber incidents over firms. Both the operational impact and the monetary costs arising from cyber incidents are heavier, due to the more sophisticated techniques employed by cybercriminals. The economic consequences of this changing scenario need to be taken into account since the impact on firms, consumers, and the real economy as a whole is already strong, but without clear and effective measures and cooperation among different actors could be harsher. For these reasons, the implementation of a comprehensive set of rules from supervisors is essential to prevent an escalation of the danger to the economy. This study aims at giving an overall image of a complex problem, by trying to represent first the general context from which the problems arise, the cyberspace, that was further crowded by the pandemic crisis that moved a lot of activities into the web. Then it wants to underline which are the economic consequences that arise and could arise from those kinds of attacks, that according to our analysis have a direct impact on the economy as a whole. As already stated, the costs of cyber-attacks are high, but according to various sources, they could erode up to 1% of the world GDP. The difficulties in quantifying precisely those costs are due to the tendency of institutions to hide the occurrence of cyber-attacks, to protect them from the loss of customers and confidence. But this problem needs to be overcome by increasing the collaboration through higher cooperation, higher investments in research and development, and higher cybersecurity measures. Moreover, institutions should aim at creating a real culture around cybersecurity issues. It is important to prepare both single customers and single firms and to make them understand that their actions do not impact only themselves and their companies, but the whole economy. In fact, according to the models we presented in the second chapter a cyber-attack not faced as it should, could lead to a situation of systemic crisis.

According to the main findings of this research, the next step in the fight against cybercrime should be based on stricter and more coordinated rules all over the world. The differences between the EU and the US are still a lot, and for a more efficient cyber response, they need to work on a stronger collaboration. Even though the various CSIRT of different countries already act as a link between the response of single countries and the European institutions, the creation of an automated response and report mechanism could limit the possibilities of escalation of cyber incidents toward a systemic event. In fact, by employing a real-time network that could warn related institutions, the operational and systemic damages could be reduced drastically. This necessity has been presented also in the review process of the NIS directive, which will lead to the development of the NIS2. This result can be achieved only through higher cooperation and coordination across the different legal frameworks.

BIBLIOGRAPHY:

ABI Lab, Cert Finanziario Italiano, (2017), Sicurezza e frodi informatiche in banca: come prevenire e contrastare le frodi su Internet e Mobile banking

Accenture security & Ponemon Institute LLC, (2019) The cost of cybercrime

Amir, E., et Al., (2018), Do firms underreport information on cyber-attacks? Evidence from Capital Markets, in Review of Accounting Studies

Banerji, G., (2019), Capital one Shares Fall Nearly 6% After Breach, in The Wall Street Journal

Bernard, J., Nicholson, M., (2020), Deloitte and FS-ISAC survey, Reshaping the cybersecurity landscape.

Boer, M., et Al, (2017), Institute of international finance, Cybersecurity & Financial Stability: How cyber-attacks could materially impact the global financial system

California Financial Code, (2003), California Financial Information Privacy Act

Link:https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=1.4.&lawCode=FIN

Carter, L., et Al., (2009), Submarine cables and the oceans: connecting the world

Centrify and Ponemon Institute, (2017), The impact of data breaches on reputation & share value

CGI and Oxford Economics, (2017), The cyber value connection

Clusit,, (2020), Clusit Annual report 2020

CPMI-IOSCO, (2012), Principles for financial market infrastructures

CSIS and McAfee, (2020), The hidden cost of cybercrime

Cybersecurity requirements for Financial Services Companies

Link: <https://govt.westlaw.com>

Decreto del Presidente del Consiglio dei ministri, (2013), Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale

Decreto del Presidente del Consiglio dei Ministri, (2014), Strategia nazionale per la sicurezza cibernetica

Decreto del Presidente del Consiglio dei Ministri, (2017), Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale

Decreto del Presidente del Consiglio dei Ministri, (2020), Regolamento in materia di perimetro cibernetico nazionale

Decreto Legislativo 65/2018, (2018), Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

Decreto Legge 179/2012, Ulteriori misure urgenti per la crescita del Paese

Decreto Legge 105/2019, Disposizioni in materia di perimetro di sicurezza nazionale cibernetica

Eisenbach, T. M., et al, (2020), Federal Reserve Staff Report No.909, Cyber Risk and the U.S financial System: a pre mortem analysis

European Banking Authority, (2018), The EBA Fintech RoadMap

European Commission, (2013), Joint Communication to the European Parliament, the Council, the European Economic Committee, and the Committee of the region

European Parliament and Council, (2015), Directive (EU) 2015/1535 of the European Parliament and Council

European parliament and Council, (2015), Directive (EU) 2015/2366 of the European Parliament and the Council

European Parliament and Council, (1995), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

European Parliament and Council, (2006), Directive 2006/48/EC of the European Parliament and the Council

European Parliament and Council, (2019), Regulation (EU) 2019/881 of the European Parliament and the Council

European Systemic Risk Board, (2020), Systemic cyber risk

Farrer, M., (2020), New Zealand stock exchange hit by cyber-attack for the second day, in The Guardian

Fazio, A., Zuffranieri, F., (2018), Questioni di Economia e Finanza, Occasional Paper for the Bank of Italy, Interbank payment system architecture from a cybersecurity perspective

Federal Reserve, (2020), Supervisory policy and Guidance Topics

Link:<https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm>

G7 Cyber Experts group, (2016), G7 fundamental elements of Cybersecurity for the financial sector

G7 Information center, University of Toronto, (2016), G7 Fundamental elements for effective assessment of cybersecurity in the financial sector

Huang, K., et Al., (2020), A cyberattack doesn't have to sink your Stock Price, in Harvard Business Review

IBM and Ponemon Institute, (2020) Cost of a Data Breach Report 2020

Ikeda, S., (2020), New legislation in the U.S Proposes Federal Data Protection Agency, Broad Range of new Enforcement Actions, in CPO magazine

Kolesnikov, O., (2018), Securonix Threat Research Team, Cosmos bank SWIFT/ATM US\$13.5 million cyber attack detection using security analytics

Kosseff, J., (2018), Iowa Law Review, Vol.103, No.985, Defining Cybersecurity Law

Legge di stabilità 2016, (2015), Disposizione del bilancio annuale e pluriennale dello stato

Lombardo, S., (2021), Cyber crime, aumentano attacchi informatici e truffe online a tema Covid-19: come mitigare i rischi, in Cybersecurity360.

Lowary, J., (2018), Three Important Things Jerome Powell Said to Congress, in Bankdirector.com

Maurer, T., Nelson, A., (2020), Carnegie Endowment for International Peace, International Strategy to Better Protect the Financial System Against Cyber Threats

Neyret, A., (2020), Stock market cybercrime

Ottis, R., Lorents, P., (2010), Cyberspace: Definition and Implications. In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited

Ros, G., European Systemic Risk Board, (2020), Occasional Paper Series No 16

Rotondo, P.L., (2020), Clusit Annual Report 2020, Finance Focus

Rushe, D., (2014), Jp Morgan Chase reveals massive data breach affecting 76m households, in The Guardian

Tosoni, L., (2020) Verso una direttiva NIS 2, che cambia le proposte della commissione UE, in Cybersecurity360

United States Congress, (1999), Gramm-Leach-Bliley Act

Verizon, (2020), 2020 Data Breach Investigations Report

Vitagliano Stendardo, A., (2010), La criminalità informatica nei sistemi di pagamento digitale e con smart card. First edition. Gedit Edizioni. Bologna

Winder, D., (2020), \$645 Billion cyber risk could trigger liquidity crisis, ECB's Lagarde warns, in Forbes

SITOGRAPHY:

Bernard, J., Nicholson, M., (2020), Deloitte and FS-ISAC survey, Reshaping the cybersecurity landscape

Link:<https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html>

De Best, R., (2020), Statista, Cryptocurrency Market Capitalization 2013-2020

Link:<https://www.statista.com/statistics/730876/cryptocurrency-maket-value/>

Financial Stability Board, Cyber Resilience

Link:<https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/cyber-resilience/>

Hall, J., (2020), A guide to the NIST Cybersecurity Framework

Link:<https://www.ifsecglobal.com>

Personal data breaches, Information commissioner's Officer

Link:<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

Reciprocity Labs, (2020), What is security by design?

Link:<https://reciprocitylabs.com/resources/what-is-security-by-design/>

Ronchi, A., (2018), Come si calcola il danno reputazionale?

Link:<https://ronchilegal.eu/2018/06/28/come-si-calcola-il-danno-reputazionale/>

Sobers, R., (2021), 134 Cybersecurity Statistics and Trends for 2021

Link:<https://www.varonis.com/blog/cybersecurity-statistics/>

Link:https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

Link:<https://purplesec.us/resources/cyber-security-statistics/#>

Link:<https://www.pandasecurity.com/en/mediacenter/news/covid-cybersecurity-statistics/>

Link:<https://www.avast.com/it-it/c-ransomware>

Link <https://digital-strategy.ec.europa.eu/en/policies/nis-directive>

Link: <https://eur-lex.europa.eu/>

Link: <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>

Link: <https://www.nist.gov/cyberframework/perspectives>

Link: <https://www.iso27001security.com/html/27001.html>

Link: <https://www.sec.gov/spotlight/cybersecurity>

Link: https://www.consob.it/documents/46180/46181/comunicato_cnsb_bi_20200116.pdf/a32d82bf-3e30-42f3-9a91-6c7ccfeeb2ed

Link: https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery