Politecnico di Torino

Master’s Degree in Engineering and Management
A.Y. 2022/2023

Cybersecurity: economic analysis and market evaluation

Supervisor:
Prof. Carlo Cambini

Candidate:
Sara Carsili

July 2023

Index

1. Introduction

Innovation and low cost of the Internet have led to an increase of its performances and availability. Businesses, governments, people and the society in general have become increasingly integrated all around the world and they mainly operate in cyberspace. A lot of aspects of people's lives are strictly linked with this space, and for this reason any instability or challenge will directly affect people. There could be various scenarios for significant damages that can arise, including a virus that spread in the financial systems and disrupt a stock market, or that enter in the network of a power plant and stop it, or even in a control system for air transports, causing incidents. It is not so easy for experts to address these risks and provide a theoretical basis for the creation of an effective framework from both a business and a legal perspective.

Today cybersecurity represents a requirement for organizations, both for avoiding monetary, reputational damages and risks for their business continuity, and for operating in current markets, especially in recent years in which the security issue has reached the general interest and consumers require a higher level of protection of their data. The threats' emergence in cyberspace worsened with the Covid-19, since it has opened the way for the remote working, making organizations even more dependent on Internet and increasing the data that are stored online.

The security of each organization is based on three principles: confidentiality, integrity, and availability. They represent the *security triangle* (CIA) that is a model designed to guide policies for information security in the companies. In particular, the *confidentiality* principle claims that the access to sensitive data has to be granted only to authorized people, while the *integrity* principle states that the manipulation of sensitive data can be done only by authorized individuals, and, finally, the *availability* principle claims that data has to be accessible to authorized people, entities and devices.

Possible targets of cyber-attacks are mainly the corporations that manage large amount of data [1] even if any firm providing products or services can be attacked and any individual could be at risk of data theft. A potential disclosure of their sensitive information can impact stock prices, affect business continuity and cause organizations' failure.

Reasons of such attacks are many, and the largest ones are related to financial gains or the willingness to create reputational damages to the firm. For this reason, cyber-investments have become central, but when they are not sufficiently effective, public policies come into play, especially for consumers data protection.

Among the general cybersecurity practices, the ones that could be implemented by each user in order to mitigate the cyber risks, there are practices such as the installation of firewall, that is a software application or a hardware enforcement that creates a wall between the user's computer and the Internet. It filters the incoming and outgoing traffic of the computer in order to identify the potential threats and safeguard the PC. In addition, it is possible to implement a honeypot, just like a flower to attract bees: these technics are used to attract the attackers with a certain system that looks vulnerable in order to defend the real system. Other techniques are the use of alphanumerical password, antivirus software and avoiding the opening of email from unknown addresses. If awareness about how to move in this space become integrated in people habits, it can bring beneficial effects also on a large scale when implemented in greater context, such as companies, by employees. In fact, human errors represent one of the main causes of cyber breaches suffered by firms.

Cybersecurity is not only theory, but it needs to be actually adopted by organizations, in order to avoid potentially large damages. Some of the largest attacks of the recent years and the relative effects are reported below:

- **SolarWinds – 2020 – Supply chain attack**

  The SolarWinds attack was very powerful due to the fact that not only an organization was breached, but the whole supply chain, affecting thousands of companies. SolarWinds is a major software company based in Okla, that bases its business in the provision to other organizations of system management tools and other product, such as an IT performance monitoring system called Orion, with privileged access to IT systems. The SolarWinds Orion system was the one chosen by attackers for the breach due to its privileged position. The method used for the attack was the supply chain attack for which the target party is not breached directly, but through an organization's system in which it has access. Indeed, SolarWinds was perfect for the attack since its Orion software was used by many multinational companies and government agencies. The hackers gained access in SolarWinds system in September 2019 and inserted malicious code into the Orion system in February 2020. On March 26, 2020, SolarWinds inadvertently delivered an update of the software with the backdoor malware inside, that was called Sunburst. Once the backdoor was created, hackers accessed the victim organizations' network and their files. The malware affected more than 18000 customers [2], including many companies and organizations. Among the ones that suffered from the breach there was Microsoft, Intel, Cisco and Deloitte.

- **Colonial Pipeline – 2021 – Ransomware attack**

  Colonial Pipeline is an American oil pipeline system based in Texas. The attack had the goal to ask for a ransom, in fact the company paid the amount requested by the attackers in bitcoins, for a value of 4,4 million $. After the payment, the hackers provided a tool to the company in order to restore the system, but it needed a long process to get back up of the system. In addition, the hacker group has stolen a huge amount of data the day before the malware attack.

  The attack made arise several concerns about the vulnerability of infrastructure, including the most critical ones. The company halted all the pipeline operations during the attack, and this caused fuel shortage that began to occur in the days after the attack and the price per gallon reached very high level. A part of the ransom paid (2,3 million $) was recovered by the U.S. Department of Justice.

- **Stuxnet – 2010 – Malware attack**

  This is the first case of cyber-attack to Operational Technology (OT) in which an hackers' group sabotaged an Iranian uranium enrichment plant, causing the centrifuges to shut down. A virus propagated in the system through an USB device and remained inside for a long period until the attackers have been able to change the centrifuges rotations with sudden accelerations and decelerations in order to destruct them. This malware looked for Windows PC in which project management software was installed, in particular the Siemens Step 7 software, for working in parallel each time the software was installed. This type of attacks shows that complex techniques as this one, with high level of knowledge, could reach also the code rewriting, making the plant out of control. The malware of this attack is well known with the name of Stuxnet.

The attacks occurred have shown how lack of awareness and cybersecurity practices are very recommended and necessary. Even the best cybersecurity methods can be bypassed by advanced hacker supported by the always better technologies. A 2017 Bank of Italy report states that even if the majority of businesses in Italy adopt cybersecurity measures (only 1.5% of businesses do not have any engagement in cybersecurity), one third of them reports at least some damages from cyber-attacks [1]. In addition, the ENISA report shows that EU organizations allocate share around 6% of their IT budget to information security, and on average they invest 41% less to information security with respect to the counterparts in the United States [3]. These results shed light on the fact that what is actually done in this field it is not still enough to minimize the risk, but it is necessary a greater effort in the investment and its effectiveness. As company grows, cybersecurity becomes less easy to manage and more investment is needed in order to manage the cyber risks with the best solutions and to the highest possible extent.

A clear and comprehensive overview of cyberspace, cyber criminals and attacks, and the applicable cybersecurity measures is fundamental in a field so complex and in continuous evolution. For this reason, there will be firstly presented the basic concepts related to cyber space and the types of hackers and attacks; after that, it will be explained how cyber risks are influenced by factors that are both external to firms and beyond their control, and the ones within firms and their choices. A subsequent chapter will present the cybersecurity investments that firms should adopt in order to minimize the cyber risk with respect to the optimal level in pricing and advertising regime, and in market circumstances in which technical and market spillovers occur. A focus on the cybersecurity measures adopted by Italian firms and the cyber risk they are subject to is presented throughout the thesis. As final aspect analysed in this work, there will be a presentation of the public policies methods that can be applied, and the ones actually adopted in United States, Europe and Italy.

2. Introduction to cyberspace

2.1. Cyber definitions

According to the definition presented by Li, Yuchong, and Qinghui Liu [4], *cyberspace* can be defined as the "Interconnected networks, from IT infrastructures, communication networks, computer systems, embedded processors, vital industry controllers, information virtual environment, and the interaction between this environment and human beings for the purpose of production, processing, storage, exchange, retrieval and exploitation of information". Thus, the cyberspace can be defined as the box in which all our virtual activities happen and where the hackers tend to manipulate and steal the information produced by our virtual activities. Information includes sensitive data, personal and private information, money, intellectual properties and so on. At the basis there is always the *information*, the engine of the whole world of cybercrimes.

Different terms have been introduced so far and need to be presented in a more detailed way: a *cyberattack* represents "any unauthorized cyber act aimed at violating the security policy of a cyber-asset and causing damage, disruption or disruption of the services or access to the information of the cyber asset." [4].
The *hacker*, instead, is "a person who enters a system without permission or who increases his/her access to information to browse, copy, replace, delete or destroy it" [4].
In such a threatened ecosystem, cybersecurity investments are critical for organizations to ensure the integrity, confidentiality and availability of data assets and corporate information, as well as the survival of the business itself. The cybersecurity indeed, includes the practical measures engaged by the system in order to protect information, networks and data against internal or external threats.

Starting on what threatens the corporate ecosystem, in the following section it is provided a better understanding about hackers' categorization, even if it needs to be continuously updated since they expand and change overtime with new technics, motivations and abilities. A detailed overview related to the types of cyberattacks more used by perpetrators until now and the emerging threats are also presented.

2.2. Hackers' skills, motivations and strategies

Historically, cybercriminals were grouped all into a general category, regardless of their actions and motivations [5]. Today, cybersecurity experts differentiate typologies of hackers and their motivations, providing a better understanding of cybercrimes and relative cybercriminals. In this section an overview about the actors and threats that it is possible to find in cyberspace will be presented in order to inspect the framework in which the following analysis are acting. However, the hackers' motivations, strategies and skills continue to evolve, and consequently the typologies identified in the past few decades have to be updated overtime.

Existing theories inspect the psychological factors that lead hackers to take a path on cybercriminal activities. The first theory to analyse is related to the model of hacker development proposed by Beveren [6] based on traditional theories of psychology and the flow construct. The *flow* is defined by Csikszentmihalyi as a sense of effortless action felt when a person is highly involved in an activity to the degree whereby attention becomes undivided, and time is obscured by the involvement in the activity [7]. Such a tendency is what leads a hacker to gravitate towards criminal behaviour as they develop their skills in this field. Accordingly, the motivations to hack were divided into four themes: 1) compulsion to hack, 2) curiosity, 3) control and attraction to power, and 4) peer recognition and belonging to a group. In addition, it is possible to consider also the Albert Bandura's theory [8] for which individuals engage in criminal behaviours through associating with criminals in personal or social groups. For the theory presented, it is probably that an individual undertakes criminal behaviour with other criminals and imitating their behaviours, if he is exposed to attitudes, norms, orientations that justify or rationalize such behaviour, and whether he has example of similar behaviour in the past that have been rewarded. Based on Rogers, 2011[9], cybercriminals would feel a need to justify their illicit activities in the form of pursuing a noble or higher cause and often this could be also justified by the positive reinforcement received from the community that often outweighs the punishment received from the real world.

As explained above, the concept of *flow* is extremely significant for a growth from an amateur to a competent hacker and only with an additional subjective tendency to commit a crime would these hackers gravitate towards cybercriminal activities. Describing hackers' motivations is useful in order to makes it possible to comprehend not only their motivations but also why a specific motivation applies to a hacker type. It is also noteworthy that hackers are represented by a community of different individuals and organizations who act under varying motivations, purposes and levels of expertise. For this reason, a categorization reported by Chng et al. [10] about the types of hackers, based on their expertise, and the motivations behind their actions is proposed below:

- **Novices** refer to hackers who have a minor expertise and rely on online tools developed and provided by others. They are also called script kiddies, newbies, and system challenges. Novices are characterized by their motivational characteristics of curiosity and recreation.
  How they act: novices usually use malware found on the Internet and Dark web that they slightly change. They attack for curiosity and test their abilities without any plan of action in terms of the attack steps to be executed to reach a specific goal. Novices act through malware installation, phishing, SQL injection. DDoS, etc.

- **Students** have no malicious intent but hack to gain knowledge and better competences. They are motivated by curiosity.
  How they act: students, as novices, use existing codes/scripts, but applying some modifications to experiment and study vulnerabilities in systems.

- **Cyberpunks** have a low-medium level of expertise and hack for fun. Alternative names for this type of hackers are crashers, thugs, and crackers. They would reach a financial gain, notoriety and recreation from attacks.
  How they act: they may use existing codes/scripts with some modifications or write their own ones. They cause damage to targeted systems, crash victim’s devices and deny legitimate users’ access. They could use DDoS attacks, phishing, spamming, SQL injection or ransomware.

- **Online sex offenders** are individuals who misuse the Internet to engage in sexually deviant behaviours. They include cyber predators and pedophiles.
  How they act: they view or post illegal pornography on the Internet, initiate sexual online chats with a child/adolescent and share sexual content. Their tactics include befriending potentially vulnerable victims on social media and getting hold of compromising pictures/videos directly or through emails/chats embedded with malicious attachments.

- **Old guards** are non-malicious hackers who include white hats, sneakers, grey hats, and tourists. They are motivated by notoriety, recreation, and ideology. How they act: old guards use customized codes and penetration testing tools to reveal vulnerabilities in existing systems such as websites, software and devices, They also find new malware and track malicious hackers using cyber forensic techniques. They may inform systems' owners about the vulnerability directly, or report the vulnerabilities to concerned companies and authorities, or decide to make the vulnerability public. In case of white hat hackers, they work with security companies and law enforcement authorities, and in other cases (e.g., grey hat hackers, sneakers), they anonymously carry out their activities.

- **Insiders** are dissatisfied employee who abuse their access. They are motivated by financial gain, revenge, and ideology.
  How they act: use internal company's knowledge (e.g., account credentials, security policies or system vulnerabilities) to launch attacks or sell that information to Dark web buyers or competitors for financial gains. They may also accidentally leak company information or infect the company's enterprise network due to lack of due diligence in browsing on company IT equipment and network.

- **Petty thieves** refer to criminals who have moved their criminal activities online and would gain in financial terms or are motivated by revenge. They include extortionists, scammers, fraudsters, thieves, and digital robbers. How they act: petty thieves use trojans, phishing and ransomware attacks which are easily available on the Internet.

- **Digital pirates**, also known as copyright infringers, they act through the illegal duplication, distribution, download, or sale of copyrighted materials. They are financially motivated.
  How they act: they steal copyrighted content and leak them using online websites, torrents, etc. For example, they could provide contents to websites that illegally stream copyrighted movies, TV shows, music, or distribute all types of digital contents.

- **Crime facilitators**, also called supporters, have specific skill sets or area of expertise and provide tools and technical know-how to cybercriminals enabling them to launch sophisticated attacks which would not have been possible otherwise. They are usually financially motivated.
  How they act: they may offer cybercrime-as-a-service to criminals by helping them carry out phishing campaigns, renting out malware (generic and customized) and botnets, renting infrastructure (bullet-proof hosting, VPN, proxy services),

launching DDoS attacks against certain targets on the criminals' behalf, providing access to personal and financial data leaked from compromised databases, hacking of email and social media accounts, and managing cryptocurrency wallets to hide illegal transactions. They operate from underground forums and websites on the Dark web which serves as markets connecting buyers and sellers.

- **Professionals** are highly skilled individuals who act as guns for hire or with the intent of increase their achievements. They are motivated by financial gain and revenge. Alternative names for them are black hats, elites, criminals, organized criminals, information brokers, and thieves.
  How they act: professionals perform sophisticated attacks potentially using all types of cyber-attacks (phishing, ransomware, SQL injection, DDoS, cross-site scripting, supply chain attack, all types of malwares, etc.) and customized codes. They have a high expertise also in not leaving any trail behind which may lead authorities to them or instead leaving clues that are meant to confuse investigators. They typically operate on their own, in small groups or with criminal organizations.

- **Nation states** are trained and high skilled hackers who work for one government to destabilize, disrupt, and destroy the systems and networks of a nation or government. They are motivated by financial gain, ideology, and revenge. This category includes information warriors, cyber terrorists, cyber warriors, state actors, state-sponsored networks, and spies.
  How they act: nation states perform sophisticated attacks following a series of stages: first, they gain access to a target network through social engineering techniques. After that, they install malware inside the network and then try to gain administrative rights. At the end they identify and prepare the target valuable data and transfer it to their systems for a long time trying not to attract any attention. They often left a backdoor open in order to perform additional access in the future. They take care to not leave their tracks and sometimes deliberately leave clues that are meant to confuse investigators. Nation states typically work in a group and coordinate with each other.

- **Crowdsources** are individuals who come together to solve a problem and perform a more sophisticated cyber-attack. They are motivated by notoriety, revenge, recreation, and ideology.

How they act: they are part of a hacking forum who join forces and pool their skills together for various tasks such as developing new malware, managing botnets, sharing network infiltration tools and techniques, and stealing financial information.

- **Hacktivists**, also known as political activists and ideologists, use their technical skills and use the Internet in order to obtain a political change or spread their political ideology. They are motivated by notoriety, revenge, recreation, and ideology.
  How they act: hacktivists often operate in a group. They use different cyber-attack vectors such as SQL injection, DDoS, social media account compromises, etc. They steal information from databases which may contain sensitive and private information. They could also disable widely used public services, send fake news or posts containing phishing/malware/trojan links to a large follower audience which can help them gain the attention of public and authorities to give publicity to their cause. They are careful to cover their tracks which may otherwise lead authorities to them.

The categorization presented above helps in the understanding of the reasons why hackers hack and what contributes to their activities. For the purposes of our analysis on the cyber risk of firms and the relative impact on the economies, a particular attention is for certain typologies of hacker, such as old guards, insiders and professionals, even if each malicious activities with a certain level of expertise in case of lack of diligence could cause damages.

2.3. Cyber-attack types

In order to have a knowledgeable overview of the cyber risks that each user and each company has to face with when it acts online throughout the daily business activities, the types of strategies and attacks adopted by cybercriminals, based on the processes used and the resources impacted, are reported below [11]:

- **Man-in-the-middle attack**

MitM method involves introducing the threat actor as a legitimate resource between two parties that could be a user and an application. Once the forced introduction in the middle of two parties has been established through the first step of Interception, the attacker gains full visibility to any online data exchange, and he can pass to the second step of decryption of the Two-Way SSL (the method for which both client and server

authenticate each other to ensure that both parties involved in the communication are trusted) without alerting the user or application.
The MitM's goal is to steal personal information, such as login credentials, account details and credit card numbers. The typical target users are all the online services in which logging in is required, such as financial applications, e-commerce sites, SaaS business and other websites.

The above-specified scenarios are not just theory. Some examples of MitM attacks occurred in the history of cybercrimes are the following:

- DigiNotar Breach (2011) has been caused by a MitM and resulted in the organization's bankruptcy. The attacker obtained around 500 certificates for top service providers (including Google, Yahoo, Mozilla, Skype, and so on) to mimic a legit site. Later, he used these certificates to trick Gmail users in Iran leading to serious troubles.
- A visual search engine named Superfish was pre-configured in Lenovo systems before 2015. The software had adware (a type of malware that hides on devices and involves displaying advertisements and it can also monitor users' behaviour as they browse so that the type of ads displayed can be adjusted) scanning the SSL traffic passing through those systems and installing fake certs on these devices. MitM attackers did eavesdropping through this adware and ran ads as per their wish – even on the pages that were encrypted. The scandal made Lenovo lose $8.3M in the lawsuit.
- Equifax Data Breach (2017) caused by a MitM, made the company take its Android and iPhone apps off the respective app stores because the organization did not use HTTPS connection (Hyper Text Transfer Protocol Secure connection for which the exchanged data with a website are encrypted. The website is protected with an SSL certification) and allowed hackers to intercept the traffic, making personal data of more than 160 million users insecure from the US, UK and Canada.

- **Advanced Persistent Threat (APT)**

An Advanced Persistent Threat (APT) represents a cyber-attack in which attacker use continuous and sophisticated hacking techniques in order to gain the access in the computer network system and to remain undetected for a significant period. In the

period between the infection and the remediation, the hacker has the possibility to collect information about network activities and sensitive data.
An APT objective is primarily to steal data and intellectual property, and, in addition, it could also develop a good knowledge of the network in order to cause Denial of Service attacks or infect the system with malware.
APTs often use social engineering tactics or software vulnerabilities in order to enter inside. Example of this type of attack include Titan Rain, Ghostnet, Stuxnet.

- **DoS and DDoS attack**

Denial of service (DoS) and Distributed DoS (DDoS) consist in making a PC or a cyber-service inaccessible by sending overflowing access requests from various sources and creating an excessive traffic on the line. Given a sufficiently high number of requests, the website's server will not be able to process all of them along with the legitimate user requests. Legitimate users will experience this as website-load delays, timeouts, and eventually not being able to connect to their desired websites at all.
In order to make larger and more complicated attacks, hackers usually leverage a network of bots, a botnet (i.e. a group of computers which have been infected by malware and have come under the control of a malicious actor). Botnets can be designed to accomplish illegal or malicious tasks including sending spam, stealing data, ransomware, fraudulently clicking on ads or distributed denial-of-service (DDoS attacks) [12]. The attacker will orchestrate the botnet to bombard the victim's websites with HTTP requests. Mainly, it is used to plan a more damaging attack in the future.

According to The Record [13], Google has been victim of the largest DDoS attack in the world in June of 2022. The attackers' requests had a peak at 46 million requests per second, which was compared to the number of requests Wikipedia receives every day. The attack lasted about 30 minutes and was caused by more than 5,000 devices from 132 countries. DDoS attack protocols and the Google security team prevented what could have been a significant security risk for billions of users.

- **SQL injection**

First of all, it is necessary to remark that data is nowadays among the most crucial parts of every information system. Hence, organizations use databases in order to properly manage these through applications on the web to get clients' information. SQL (Structured Query Language) is a famous query language used to gather and oversee

data in a dataset. The SQL injections attacks are made through the SQL-based ill-intended codes entered in the vulnerable systems and applications. Once the code has been successfully introduced, a SQL injection can collect the query results, give new commands to the systems, and perform prohibited actions on success. SQL injection vulnerabilities are often used by attackers to pass security checks of the challenged applications. They will gather all content from the structured language database by transferring permissions and validating web server web applications or website pages. SQL Injection also allows attackers to add, edit, and delete notes from the database and gives attackers access to confidential client data such as private information, licensed inventions, and proprietary benefits, among other things.
SQL additionally allows attackers total control of the database. For example, in a monetary web application, an attacker could utilize SQL injection to adjust account balances, move cash to another account, or void exchanges. In exceptional cases, it is possible to execute commands in the operating system leading to potential severe consequences.

Real SQL injection attacks are reported below [14]:

- GhostShell attack: hackers from APT group Team GhostShell targeted 53 universities using SQL injection, stole and published 36,000 personal records belonging to students, faculty, and staff.
- Turkish government attack: when another APT group, RedHack collective, used SQL injection to breach the Turkish government website and erase debt to government agencies.
- 7-Eleven breach: a team of attackers used SQL injection to penetrate corporate systems at several companies, primarily the 7-Eleven retail chain, stealing 130 million credit card numbers.
- HBGary breach: hackers related to the Anonymous activist group used SQL Injection to take down the IT security company’s website. The attack was a response to HBGary CEO publicizing that he had names of Anonymous organization members.

- **Zero-day exploit**

Zero-day exploit consists in cyber-attacks that take place by taking advantage of any hardware/software weaknesses that is unknown by engineers in the moment of the attack. While the weakness is open, attackers can compose and carry out a code to exploit it. This is called *endeavor code*. When a zero-day weakness is recognized by malicious users, they need a method to reach the weak framework.

Typical attack vectors include Web browsers, which are common targets due to their ubiquity, and email attachments that use vulnerabilities in the application opening the attachment, or in specific file types such as Word, Excel, PDF or Flash. Opening such files, the aggressor's malware invades the client's documents and information. The "zero-day" term is used since engineers had zero days to fix the imperfection before the weakness was misused or diffused to the society knowledge. Such attacks have a high probability of success because defences are not in place. The intensity of 0-day attacks is generally low in the beginning and lasts for longer.

Zero-day vulnerabilities are valuable for different parties, in fact there is a market in which organizations pay researchers who discover vulnerabilities (white market). In addition, there are grey and black markets in which zero-day vulnerabilities are traded, without public disclosure, for up to hundreds of thousands of dollars [15].

As victims of a zero-day exploit attacks we can report:

- Sony Pictures: the attack in 2014 paralysed Sony's network and led to the release of sensitive data on file-sharing sites. Details of forthcoming movies, business plans, and the personal email addresses of senior Sony executives were among the compromised data.
- RSA: in 2011, hackers used a vulnerability in Adobe Flash Player to gain access to the network of security company RSA. The attackers sent emails with Excel spreadsheet attachments to RSA employees. The spreadsheets contained an embedded Flash file that exploited the zero-day Flash vulnerability. When one of the employees opened the spreadsheet, the attacked installed the Poison Ivy remote administration tool to take control of the computer. Once they gained access to the network, attackers searched for sensitive information, copied it and transmitted it to external servers they controlled. RSA admitted that among the data stolen was sensitive information related to the company's SecurID two-factor authentication products, used around the world for access to sensitive data and devices.

- **DNS Tunneling**

Domain name system, or DNS, is the protocol that translates human-friendly URLs into machine-friendly IP addresses. DNS is a critical and foundational protocol of the internet. It is often described as the "phonebook of the internet" because it maps domain names to IP addresses. DNS tunnelling attacks exploit the DNS protocol to tunnel malware and other data through a client-server model. The attacker predefines a domain whose domain's name is related to the attacker's server, where a malware program is installed. Because DNS requests are always allowed to move in and out of the firewall of a company, an attacker's infected computer is allowed to send a query to the DNS resolver, a server that relays requests for IP addresses to root and top-level domain servers. The DNS resolver establishes a connection between the victim and the attacker by routing the query to the attacker's command-and-control server, where the tunnelling program is installed. This tunnel can be used to get data or for other malicious purposes. Because there is no direct connection between the attacker and victim, it is more difficult to trace the attacker's computer.

DNS tunneling that has been used in past years are the Morto and Feederbot malware. Recent tunnelling attacks instead include those from the threat group DarkHydrus, which targeted government entities in the Middle East in 2018, and OilRig, which has been operating since 2016 and is still active.

- **Social engineering**

It is a type of cyber-attack based on the psychological manipulation of the target rather than technical expertise. This technique is used most often for intrusions and has a very high success rate. Social engineering is the term used for a broad range of malicious activities based on human interactions and leveraging human errors. All these activities have common steps: a scammer firstly investigates about the background information of the target victims. After that the attacker search for the way in which obtain victims trust and convince them to make actions in order to break security practices such as reveal sensitive information or grant access to critical resources. Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved.

Phishing is one of the ways in which social engineering occurs. It involves using emails containing corrupted attachments to steal sensitive information. Perpetrators send tempting emails to lead the victims to click on a particular link and share details like credit card details, bank info, credentials, and many more. The emails are created in a such detailed way that it seems they have come up from trusted sources. Phishing accounts for nearly half of the total cyber-attacks happening in the world.[16] An attack can have significative negative consequences both for individuals, who could suffer of unauthorized purchases, the stealing of funds, or identify theft and for companies, that could be subject to severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

- **Malware**

The term 'malware' was coined by Yisrael Radai, a notorious security researcher during the 1990s. Malware represents malicious software used to infect individual computers or an entire organization's network. It exploits target system vulnerabilities in order to enter in the network identified by the attackers and spread inside. The malware used for these attacks is of various types, e.g., Trojan, spyware, worms, and ransomware. A malware infiltration can have significant consequences that include data theft, extortion or the crippling of network systems.

Before the advent of the Internet, the malware was used to reach the targeted system with the help of software, drives, CDs, and floppy disks. In the 1990s Internet amplified malware spread and penetration. In those years Macro viruses impacted several copyrighted Microsoft Office products. Throughout the 1990s the types of malware increase and became more sophisticated. In the 21st century, malware has become smart, resilient, and robust enough to bear any security protocols. Their frequency and impact factors have increased exponentially so much so that every 39 seconds, a cyber-attack takes place, and most of them involve malware download or insertion. [17] Several subcategories of malware exist, and among them it is possible to find ransomware, worms, and trojans.

A **ransomware** attack consists in threatening the target individual to leak or publish the crucial information on the public domain in the case in which requested ransom amount is not paid. This type of cyber-attack starts with the installation of the ransomware in the targeted victim's system that encrypts the stored data on a computer and/or across a network and forwards it to the hacker. After that, a popup display informs the user that if the ransom is not paid, the data remains encrypted, made public or lost. Some of the most common ways to introduce ransomware are phishing, adware, and USB drives. An advanced type of ransomware has recently appeared. It is called **ransomware as a**

service (RaaS) and is executed by exploiting an existing licensed malware; in case of success, a percentage of the ransom goes to the malware author.

Another type of malware includes **worms** that were originally designed to infect a computer, clone itself, and then infect additional computers via another medium, such as email. Perpetrators use worms to create botnets from a large number of compromised connected devices. *ILOVEYOU* is a worm deployed through a social engineering attack that infected 45 million computers. [18]

A **Trojan** instead is a type of worm that appears legitimate but carries with it a dangerous payload. It doesn't replicate itself as do worms, but it typically comes together with additional malware types such as backdoors, rootkits, ransomware and spyware. The world has been under attack by malware multiple times. Regin, a Trojan horse, affected many UK residents and US and did extensive monitoring. Thanatos malware was aimed directly at Bitcoin. Locky malware infected more than 5,000 systems per hour in Germany alone.

- **XSS attacks**

Cross site scripting (XSS) is a common attack vector that injects malicious code into a vulnerable web application that is activated each time a user visits the website. XSS, differently from other cyber-attacks such as SQL injections, does not directly target the application itself, but the users of the web application by compromising user accounts, activating Trojan horse programs and modifying page content, misleading users into giving their own data. Also, session cookies could be stolen, allowing scammer to impersonate valid users and use their account for their malicious purposes. A successful cross site scripting attack can have strongly negative consequences for an online business's reputation and its relationship with its clients.

Most of the cyber-attacks are planned to gain in monetary terms or to gain information and business intelligence. By obtaining passwords, access information or all possible types of sensitive information for a company, hackers would also control a specific business or enterprise to show their supremacy. Some cyber-attacks also took place because of political reasons. Hacktivism is an example of cyber-attack that is based on spreading political awareness to the public. For instance, WikiLeaks, the international non-profit organisation that publishes secret governmental and firms' documents provided by anonymous sources. It is based on cyber-crimes activities against political organizations to bring corruption, internal conspiracy, and many other issues to the public domain. Some cyber-attacks are also driven by personal motivations against a person or an organization, for instance from an employee in particular negative cases of malcontent. Among these types of cyber-attacks, it is possible to find the ones performed by white-hat hackers, involved in good-intent hacking, carried out for testing the defence mechanism of an organization. Sometimes, hackers carry out a cyber-attack just because data was available, or the end-user is not aware of best security practices. They use this opportunity to test their skills, try their hand on the new hacking skill, and show their supremacy following the flow concept explained above.

A point on which it is necessary to focus is that organizations targeted by hackers are the one that offer the higher payoff compared to the costs and risks they have to face with in making a cyber-attack. From this perspective, the biggest organizations that manipulates the highest amount of data are the ones with the major risk to be targeted [19]. Indeed, the core, or better, the engine, of all the cybercrimes functioning is the *information*. It is possible to notice that in the definitions overview reported above *information* is the basis for all the cyber definitions.

2.4. Emerging cybersecurity threats

Due to the persistent development of new technologies that are becoming even more integrated in people's lives, new threats in cyber space are always evolving too. ENISA, in its report published in March 2023 [20], has identified the cybersecurity threats that will increase in prevalence by 2030. Many of today's threats will remain, but they could change in some of their characteristics due to the possible greater dependencies and to the additional complexity that now it is not still possible to understand. The objective is to begin preparing to ensure security with respect to the new emerging threats. The top ranked threats identified by ENISA experts are the following ones [20]:

- **Supply chain compromise of software dependencies**: it has been analysed that by 2030 the markets will require always quicker product release cycles, and this will lead to the necessity of component-based programming that will reuse code or open-source code libraries. This could cause unmonitored interactions and consequent novel vulnerabilities that it is not so easy to foresee. Malicious actors will have in this way more opportunities to damage the supply chain from both supplier and customer side. The types of attacks could rank from malware injections in code libraries to phishing attacks. Due to the global size that could reach supply chains, this type of attack could cause issues at global level and can be used for espionage, financial gains or political disruptions.

- **Advanced disinformation/influence operations campaigns**: in 2030 attackers could have the capabilities for expanding their disinformation efforts to manipulate communities. Techniques such as the deepfakes that can create unreal faces that seem real for human eyes, can be used to impersonate the target. Therefore, realistic avatars could be used as bots of the future for influencing elections or public trust by sharing videos and participate visibly in public debate. AI text or voice could reinforce this technology in order to provide personalized responses to individuals. The primary reason for disinformation campaigns is political and these types of threats could be indeed conducted by politically motivated attackers.
- **Rise of digital surveillance authoritarianism/loss of privacy**: the actual technologies of location tracking, facial recognition and public cameras, in the future could be widely use leading to reduction of individuals' privacy. The access to this data could be seen as a target by attackers in order to sell them online. Private corporations that provide facial recognition technologies or content platform could be targeted for this reason.
- **Human error and exploited legacy systems within cyber-physical ecosystems**: IoT will permeate large parts of the systems from transport, industrial infrastructure, power and water grid in order to improve efficiency and decision-making. In addition, there will be an increase in the number of smart devices that people will use, leading to difficulties in the management and maintenance of them. End-users could not be educated in the smart devices' use due to lack of training and knowledge. Together with delayed maintenance, misconfiguration, attackers may use techniques such as the Generative Adversarial Networks (GAN) to reduce detection rate of cyberattacks. The situation as described can lead to risk of interception of data between devices or outages. The end-user can use smart devices for creating communication among them and mobile applications, touching their home, transport and so on. The attackers can get access in the communication channels and move to the network. Looking at the industrial systems, the access could be gotten through employees by social engineering attacks and move after in the network to find and attack industrial control systems. In addition, attacks could exploit transient cyber assets including those from third parties.

- **Targeted attacks enhanced by smart device data:** the use of smart devices in people lives will increase by 2030. Data about all aspects of life, including health information from medical equipment or wearable devices, behaviours at home, movements and interest by research online, will be collected, creating a behavioural profile for each user that can be accessed by attackers in order to exploit them for social engineering attacks. Smart devices will be often use by malicious actors online due to the lack of security that characterize them for end user low awareness and the huge number of available devices that will be used by each person and that represent, as consequence, a huge number of opportunities of attack. The initial access can be obtained through unpatched devices connected to the Internet. The attackers will gather information like credentials, identity, contacts in order to move towards more sensitive information and access financial assets or sell information on the financial markets.
- **Lack of analysis and control of space-based infrastructure and objects**: by 2030 the space sector will be more developed and integrated between private companies and governments in the pursuit to explore the universe, leading to more competition in space from geopolitical and commercial perspectives. This new sector is emerging and is object of security concerns due to the fact that there is still lack of understanding and control of space infrastructure. This could lead to exploitation of unknown vulnerabilities (zero-days attacks) to the difficulty to timely prepare for their identification. In addition, markets are going towards a fast innovation, but lowering the expense for cybersecurity. In this scenario, private companies may sabotage rivals and governments may exploit these vulnerabilities to create a competitive advantage in space, while criminal groups may use them for extorting companies for financial gains. The access could be gained through infrastructure and private actors that interact with it, or through supply-chain attacks, with the objective of maintaining their presence in the base stations, the terrestrial hub that connects the satellite to a network.
- **Rise of advanced hybrid threats**: cyber-attacks are evolving, and they are usually combined in order to be matched with offline attacks. The hybrid operations increase attacks complexity and are more difficult to detect because detection tools need more capabilities in order to correlate seemingly unrelated events, increasing the challenge for governments, companies and individuals. Attackers could use AI and deep learning in order to increase efficiency and, in particular, create new techniques

that are unforeseen and difficult to detect. In addition, the increase of smart devices, create a growing variety of opportunities that could be exploited for malicious activities.

- **Skill shortage**: the skill shortage creates today and in the future problems for security issues increasing risks to society and governments. One factor that will impact the situation will be the willingness of organizations to expand their staff. The lack of skills and maturity of cybersecurity features will also influence the implementation of cybersecurity measures, even if there will be willingness to adopt them. The workforce could not be trained for the use of new technologies interacting with legacy technologies. Criminals will target companies that have a lot of unfilled cybersecurity jobs, that would be necessary in order to manage the risk of the increased number of smart devices, artificial intelligence and space-based infrastructures or quantum computing, and they will exploit vulnerabilities for financial gains. Attackers will have access by analysing the potential vulnerabilities and opportunities to exploit.
- **Cross-border ICT service providers as a single point of failure**: All infrastructures will be significantly dependent on ICT service providers for connections and management of connections between devices. ICT service providers will represent the basis for society and therefore they could be a single point of failure. Attackers could exploit vulnerabilities in their infrastructure, getting access to their networks, or data centres, applying hybrid attacks. Due to the fact that ICT providers will connect a lot of critical services, it could be targeted in order to scale damages along the connected systems.
- **Abuse of AI**: AI is emerging and is gaining a lot of applications today, leading to a widely and powerful use in the future. It is subject to the potential threat of intentional manipulation of AI algorithms and data, training it to take incorrect choices. There could be a high risk in case of decisions-making process in critical sectors, in which the power of AI could be harmful for the society and infrastructures. Attackers could for example create dysfunctional AI applications for criminal purposes, such as the analysis of user behaviours data to create phishing or hybrid campaigns. AI can be also use for creating disinformation, collecting sensitive data, military robots etc.

3. Firms' exposure to cyber-risk

The most relevant cyber risks determinants from the firm side will be touched in this section and in particular there will be a separation between the factors external and internal to firms. They respectively refer to the ones beyond the firm's control that affect the intensity and distribution of cyberattacks, and the ones that differ from company to company. In the former case there will be a focus on the geographical distribution of cybercrimes, socioeconomic status influences, digital infrastructure role in creating complementary assets for cybercrime and, finally, the online users' behaviours and the related privacy paradox they are subject to. In the latter case are firstly analysed the different cloud storage systems that firms can adopt (centralized vs decentralized systems) and how this choice affects their cyber risk; in addition, the influence of perceived attractiveness, Internet presence and organizational countermeasures have been analysed in order to understand their incidence on cyber-attacks. The topics are explored in depth due to the consequences that involve on the cyber risk.

3.1. Factors external to firms

Even though cybercrime is acquiring prominent importance being one of the most salient negative impacts from the Internet, a lack of theorization is evident at the present time. It would be necessary the development of a theoretical framework in order to better manage and control it.

The study performed by Jiyong Park et al. in their article published in December 2019 [21] tries to cover this gap by inspecting the correlation and interconnection existing between cybercrimes and factors such as geographical distribution of cybercrimes, socioeconomic status and the broadband role. These factors that influence the cyber-risk are external to companies and beyond their control, and, as consequence, not easily manageable. Despite that, a better understanding of them and how they are correlated can help having a more conscious attitude about it.

The study conducted [21] takes as basis the comprehensive state-level data and time-varying attributes in the United States during the period 2004-2010 and examines which factors are associated with the occurrence of cybercrimes.

The analysis firstly makes a comparison between cybercrime and terrestrial crimes (violent crimes and property crimes) by looking at the geographical distribution and the motivating factors. The study based this first part of the analysis on the idea that cybercrime is different from the terrestrial one in terms of skill required, but at the same time it seems to have similar motivating factors with violent crimes since both may satisfy a psychological urge. In the second part it has been analysed that cybercrime not only requires a skilled perpetrator, but also a capacity-building infrastructure with high-speed connections to facilitate the cybercriminal activities on the web. This is linked with the idea that at the basis of cybercriminal offenses there is an economic inequality, providing evidence that the social cost that impacted violent terrestrial crime, now impacts also cybercrimes.

The study is focused on the conditions under which cybercrimes are more likely to occur. The model used is reported below:

$$ln\ (Cybercrime\ Perpetrator_{sit}) = \alpha + \beta\ ln\ (Internet_{it}) + Z_{it}\gamma + v_i + \mu_t + \varepsilon_{it}$$

where Z_{it} is a set of control variables including crime-related, demographic, and socioeconomic factors; v_i represents state dummies to account for time-invariant state-level factors such as the established state laws or regulations; μ_t represents year dummies in considering the average time trends across states; ε_{it} represents a random error. The identification in the main model arises from variations in Internet penetration and cybercrime perpetrators within states, after netting out country-wide time trends. It has been also added the interaction term between the focal-independent variable ($ln\ (Internet_{it})$) and socioeconomic factors. In fact, it is assumed that cybercrime is a computer-mediated illegal activity that occurs in the globally extended network and, as consequence, Internet penetration allows them to spread rapidly and to have greater effects.

By looking at the framework on which the study has been performed, it is possible to analyse different factors interconnected with cybercrimes, such its geographical distribution, socioeconomic status and broadbands roles.

3.1.1. Geographical distribution

Referring to terrestrial crimes, they usually occur close to criminals' home, while in cyberspace, a perpetrator can engage in illegal online activities without leaving home. In the latter case the constraint of the physical distance comes less and instead Internet can act also as a "force-multiplier" by helping individuals to produce negative effects with the minimum of resources.

In addition, as reported by Bakos and Brynjolfsson on 1999 [22] the advent of information goods with low marginal costs thanks to Internet has led to the emergence of economy-of-scale strategies in Internet businesses. Similarly, malware or others malicious software represent a type of information good with low marginal cost, leading also in this case to economies of scale and making the distribution of cybercrime activities more concentrated than that of terrestrial crimes. The study performed makes a comparison between the geographical distribution of cybercrimes and the terrestrial crimes' one. Thanks to the analysis performed it has been inspected that the degree of concentration of cybercrime perpetrators is significantly higher than that of violent crimes in terrestrial world, and the geographic distribution of cybercrime victims is more flattened across states than that of violent crimes. J. Park et al. [21] interpret these findings as a sign that cybercriminal activities could be conducted by a small number of perpetrators who are force-amplified by the Internet itself and victims could be everywhere due to the ubiquity of the Internet.

3.1.2. Socioeconomic status

In this section a particular focus is on the relationship between cybercrimes and socioeconomic status (i.e. education rate, inequality, poverty rate, and unemployment rate), by comparing it with the terrestrial crimes. With respect to the latter, the literature considers the property crimes as crimes of wealth more responsive to economic incentives and well explained by the economic theory of crimes [23], while violent crimes as crimes of impulse that are better clarified by the social disorganization theories.

Focusing on cybercrimes, they are as similar as different from terrestrial crimes. In particular, the cybercrime usually requires a high level of skills and expertise on technical field [24] linked to high educational attainment. The high skill level can increase the returns on cybercrime and outweighs the opportunity cost of crime. This leads to a direct correlation between **education** and cybercrime, that is different from the conditions of terrestrial crimes.

An additional relationship between crimes and socioeconomic status is related to the inequality and frustration that people in the lower classes feel by seeing the others' success. This feeling could result in violent crimes, which, accordingly to Kelly [23] are more related to **inequality**, while property crimes are associated with **poverty**. The framework analysed can be applied also in the virtual world, by looking for example at the cybercriminal activities carried out by a company employee for revenge. More generally, Kshetri [25] argues that a feeling of vindication against a symbolic enemy can provide a psychological benefit to the cybercriminals.

Raphael and Winter-Ebmer [26] say that **unemployment** has a positive impact on property crime rates due to the lowering opportunity cost of crime, but not on violent crimes. The opportunity cost of participating on criminal activities is determined by the probability of apprehension and conviction together with the labour market conditions, but due to the anonymous online environment, the probability of apprehension and conviction decreases and lowers the total opportunity cost of committing cybercrimes.

By considering each socioeconomic status variable (education rate, inequality, poverty rate, and unemployment rate) separately in the model used by Park et al.[21], one of the most relevant findings is that cybercrime perpetrators are likely to increase with Internet penetration in highly educated areas, implying that the high level of skills requested for these types of cybercriminal activities is fundamental. In addition, the relationship between Internet penetration and the number of cybercriminals is positively moderated in case of higher economic status (i.e. higher income and lower poverty rates). Different findings are related to unemployment rates instead. In case of high degree of inequality socioeconomic condition, it has been observed a positive relationship between Internet penetration and cybercriminal offenses.

3.1.3. The role of digital infrastructures

As Information and Communication Technologies (ICT) are becoming fundamental for firms, the access to high-speed connections has become a central topic in the policy discussion [27]. The availability of an advanced digital infrastructure, such as a high-speed broadband network, may influence firms' exposure to cyber-attacks since it provides better conditions to engage malicious activities online. Furthermore, a good digital infrastructure can play an important role in increasing the influence of socioeconomic status on the relation between Internet penetration (i.e. broadband) and cybercriminal offenses. As example it is possible to think about the reinforcement that broadband could give to the skill premium of cybercrime and the consequent higher positive relationship that educational attainment leads between Internet penetration and cybercriminal offenses.

The estimation results of the study performed by Park et al. [21] that has been conducted by dividing Internet into broadband and narrowband and analysing the different effects of Internet speed on cybercrimes, confirms that broadband amplifies the effects of socioeconomic status on cybercriminal activities.

The findings also show a positive correlation between the number of cybercrime perpetrators and the Internet connection based on advanced communication technologies (i.e. broadband), differently from narrowband that instead does not have significant relationship with cybercriminal offenses. As consequence, it has been concluded that cybercrime has necessity to have a high-speed Internet infrastructure that, in addition, increases expected benefits to commit cybercriminal activities. In other words, a higher broadband connection provides better conditions and higher returns than expected to cybercrime perpetrators.

In this study there is no clear empirical evidence that Internet penetration is significantly and directly associated with the number of cybercrime perpetrators; however malicious offenses on the virtual world may not be influenced merely by the degree of Internet penetration, and they could be contingent upon other conditions such as connection speed and socioeconomic factors. Specifically, higher education, higher income, lower poverty rate, and greater inequality are likely to make Internet penetration more positively related to the number of cybercrime perpetrators, which differs from the conditions in which terrestrial crimes are committed instead. Furthermore, broadband connections are significantly and positively more associated with the number of cybercrime perpetrators than narrowband connections, and this amplifies the moderating effects of socioeconomic status, highlighting the dark side of the advanced information and communication technologies (ICTs).

3.1.4. Consumers’ risky behaviours (privacy paradox)

With the emergence of the Semantic Web that nowadays plays a central role for billions of people around the world, the access to information has reached the unlimited extension along with the social network connectivity and the large scale of data aggregation. Simultaneously, the advent of big data and digital technologies has also led to privacy and security issues. as one of the most significant concerns of Internet users. In a 2009 study, Turow et al. [28] find that 66% of Americans do not want to be subject to tailor advertisements based on their preferences, and 86% of young adults do not want it if it means that their online behaviours are traced. In a 2015 report, the Pew Research Center finds that 93% of US adults believe that being in control of who can get information about them is important, but only 9% of them think that they have an actual control on how much information is collected about them and how it is used [29]. At the same time, as they profess their attention to their privacy, most consumers remain avid users of information technologies that track and share their personal information with unknown third parties. There are empirical evidence for which individuals are willing to trade their personal information for relatively small rewards [30]. The apparent inconsistency between the expressed attention about their privacy (privacy attitude) and the actual behaviour of users (privacy behaviour) is a phenomenon known as the *privacy paradox,* term coined by Brown on 2001 [31] and that represents the dichotomy of information privacy attitude and actual behaviour of users as they claim to be concerned about their privacy but their actual online behaviours don't really protect their privacy [32], [33]. This can be linked with the concept expressed by Grobler [34] for which in case of access of computer-illiterate users to the Internet, the lack of IT know-how can be exploited by malicious users in order to engage in cybercriminal activities. This is due to the fact that innocent web surfers can visit and disclose their personal information without knowing the privacy-related risks.

This users' attitude could strongly affect the companies' cyber-risk, since the central focus of cyberattacks are data and the relative data aggregation and the intensity of it could cause a particular attention from cyber perpetrators in order to target specific entities for the information they have. A specific focus on perceived attractiveness of firms based on the data they have is developed below in this chapter.

Acquisti on 2004 [35] argued that users' privacy-related decisions are subject to incomplete information, bounded rationality and psychological biases, such as confirmation bias, hyperbolic discounting and others. Trying to give an interpretation of the privacy paradox, it is reported the theories' distinction made by Kokolakis on 2017 [36]:

- **Privacy calculus**

  Based on the privacy calculus theory, individuals perform a privacy trade-off calculus in which they compare the expected loss of privacy and the potential gain of disclosure [37], [38], [39]. As consequence, it is assumed that individuals disclose personal information in the moment in which they find an expected gain overtakes a potential loss. Social media services have amplified the tendency by enabling a culture of disclosure: disclosure of one's activities, location, emotions, work. These technologies seem to leave privacy choices in the hands of consumers, but they don't have enough awareness and technical knowledge that is required to protect their personal information [40].

- **Cognitive biases**

  At the basis of the privacy calculus theory there is the idea that individuals take decisions as rational agents in the trade-off comparison between risks and benefits. However, Acquisti and Grossklags [41] study that human decision-making process is affected by cognitive biases. It is assumed that also privacy-related decisions are included.

  There could be an *optimism bias* that refers to the individuals' tendency to think that they are subject to less risk compared to others. Baek et al. [42] confirmed that people perceived their own personal online privacy infringement as something less impacting with respect to the others' one and they also found that optimism regarding online privacy risk lead people to not adopt privacy protective behaviours.

  An additional cognitive bias experienced by individuals online is the *overconfidence* in their skills and knowledge as shown in the study of Jensen at al. [43]. This obviously lead to underestimate the privacy-related risk and hinder from protect themselves.

  Individuals also have the tendency to discount future benefits, i.e. to value future benefits less than present ones. This tendency is related to the *hyperbolic discounting theory* [44] that claims that the humans' preferences change as they approach the time to choose among options, leading to discount the future in a time-inconsistent manner. Under this view, individuals have the intention to adopt a privacy-protection strategy by considering and comparing both benefits of privacy protection and benefits of information disclosure; however, in the decision process, they are thinking about decisions to be taken in the future. As consequence, in the moment of the actual decision, they discount the benefits of privacy protection leading to see as more beneficial the information disclosure.

- **Bounded rationality**

  In the decision-making process people don't have access to all necessary information in order to make conscious choices and considerations about the trade-off involved in the privacy decisions. Exploiting the commercial value of data can often lead to costly practices for consumers such as, price discrimination in retail markets, quantity discrimination in insurance and credit markets, spam, and risk of identity theft [40]. Thus, their decisions are affected by incomplete information and bounded rationality [32]. The latter is represented by the cognitive limitations – both knowledge and computational capacity – that individual face with. Due to the unawareness caused by incomplete information, eventual risks cannot be properly evaluated by users that could not act rationally and maximizing benefits. This implies that users don't have an appropriate knowledge about privacy protection, at both the technological and legal levels [45], leading to a leakage in privacy risk perception. Furthermore, individuals are unable to calculate the consequences of data disclosure, and this leads to neglect relative cost and prefer the benefits.

The privacy paradox phenomenon and the relative interpretations are presented in order to give an explanation of the reasons why individuals don't adopt online behaviours in order to protect the privacy concern that claim to have.

Due to the privacy issues raised up after the emergence of the semantic web, privacy regulations have been considered necessary by the Governments perspective. The General Data Protection Regulation (GDPR), that will be deeply discussed in Chapter 5, was passed in April 2016, and came into effect in May 2018 across the EU. Despite the privacy paradox phenomenon, when the greater awareness about privacy concerns occurs, users show the tendency to adopt more protective online behaviours.

This phenomenon is explained by Congiu et al. in their studies focused on the understanding of the consequences of GDPR on website traffic [46]. After the GDPR implementation, it has been documented an overall average traffic reduction of 15% in the long run. Paid channels, that are the ones that generate remuneration to third parties or deriving from internal marketing campaign, are the mostly affected by the GDPR. Unpaid channels are also affected by it: a reduction in visits has been observed, suggesting a change in users' online behaviours and showing a reduction in online advertising efficacy.

Congiu et al. [46] also studied that the user engagement with websites was significantly reduced after the GDPR adoption: in particular it has been estimated a reduction in average visit duration and the number of web pages visited, and an increase in website bounce rate, i.e. the share of users that leave the web page almost immediately after arriving on it.

The study also argues that there is an inverted U-shaped relationship between website size and the traffic reduction due to privacy regulations. This means that smallest and largest websites are the most affected by the reduction, while the medium-sized websites remained unaffected and may even grow.

The results found in this study may be the result of a greater awareness raised around the GDPR implementation.

3.2. Factors internal to firms

The factors that most affect the firms' cyber risk from an external perspective have been analysed in the previous section and refer to the ones that are beyond the firms' control, and at the same time that strongly influence the intensity of cybercrimes.

In this section, instead, there will be a focus on decisions taken by organizations that characterize their business model, and that can have consequences on cyber risks too.

3.2.1. Cloud storage services: Centralized vs decentralized system

People tend to frequent services, websites, online shops and social networks that are already widely used, based on the principle of *network externalities*. Metcalfe's Law claims that the value of a network is proportional to the square of the number of nodes. This implies that higher the number of users and higher the reward for interconnection is, leading to greater corporate values to be the ones of the most frequented places. The cumulative result of a great number of single choices is represented by concentration on different points such as operating systems, protocols, specific e-commerce sites, social networking sites, cloud computing services and so forth. The tendency towards market concentration has consequences (redistributive and accentuating effects) [19] on cyber risk, and in particular at every level of cyber risk (threat, vulnerability and impact).

Before analysing the interconnections between cyber risk and market concentration, it is necessary to define them.

With respect to cyber risk, it is a function of threat, vulnerability and impact [47], [48]. The *threat* represents the probability that a company is chosen as the target one for a cyber-attack and it range from 0% (not attacked) to 100 % (attacked). The *vulnerability* instead captures the variance related to the intrusions attempts that fail and the ones that succeed, by assigning a probability that the targeted company have a successful defence given both the attacker skills and defender ones, with a range from 0% (attackers' attempts always fail) to 100% (attackers' attempt always succeed), The *impact* instead represent the monetary, reputational, and other costs incurred after a malicious attack. These three components multiplied provide the level of cyber risk for an organisation.

For what concern market concentration, it can be measured by the Herfindahl-Hirschman Index (HHI) that represents the sum of the square of each organisation's market share. The result is a number from 1 (perfectly competitive system) to 10.000 (perfect monopoly). Markets with an HHI measure above 2.500 are considered very concentrated [19]. Concentration has several benefits, in fact bigger firms can leverage their size to capture higher return to scale and scope, improve efficiency thanks to greater specialisation, make long term investments to maximise revenue and profit growth and so forth. At the same time too much centralisation and concentration could cause economic disadvantages. Focusing on the potential security consequences it is possible to understand that in case of concentration of users, the reward from a cyber breach is higher since the user base increases [19].

Geer et al. developed a theoretical reasoning on 2020 [19] in which they try to understand the possible effect of market concentration on the different components of cyber risk, as the Internet ecosystem becomes more concentrated in the recent years and cyber risk moves towards these major hubs.

Starting from the ***threat*** component of the risk equation, as explained before, it represents the probability that a malicious user tries to compromise a target system. The analysis performed shows that market concentration changes the space in which malicious actors operate, because the higher size and network centrality of an organization influence the potential reward for cyber perpetrators that will consider the major hubs as the ones with higher rewards. In this sense the market concentration has a *distributional effect* on the threat component of the cyber risk, thus concentration leads to risk transference. The implication is that, as market concentrates, the risk to be targeted is higher for big organizations rather than small, less central ones. The latter could not be able to incur in the financial costs necessary to obtain a greater level of cybersecurity, and for this reason the transference of risk to biggest organizations could be a good tendency for small ones also in terms of positive network externalities, but they might also increase their cyber risk in this way.

Now we focus on the effects of concentration on ***vulnerability***, that captures the variance in the attack attempts' results due to the fact that attacks type, sophistication and skills of attackers vary overtime, together with the organisational defences, leading to different volumes of successful and failed intrusions in companies' networks. Market concentration has three different effects on the vulnerability component:

1. **Positive effect due to professionalism, scale and security**

   Market concentration can allow individuals and organizations to reduce their cyber risk by using professional concentrated services because the latter can often be better in providing security services than smaller firms that usually have an absolute lower investment on IT security. A higher level of security could be reached by transferring security provision to larger organizations, since professional services can provide better results than what can do individuals or small entities on their own. In this case, market concentration has a positive effect, leading to a higher level of cybersecurity for smaller firms. In addition, market concentration is an effective driver of improved malware identification; for instance, in an AV company there is a greater ability to identify emergent problems if more users or sensors are in the AV company network, leading to a better level of security. A similar case is about the spam filters in Gmail that is enabled by using the significant user base or the CDNs (Content Delivery Networks) that have greater capacity to deal with network traffic and can provide better protection if the CDN is larger. In this view, individuals can reduce their cyber risk by relying on concentrated firms.

2. **Negative effect due to the repeated attacks to bigger firms**

   The market concentration effect on threat component, for which the biggest organizations are more targeted than smallest ones, leads to consequent effects on vulnerability component too. Bigger nodes can be targeted more often, leading to vulnerability across a large sequence of attacks. By considering that the more concentrated organizations – those with a lot of users, clients, incoming links, etc. – are targeted by cyber perpetrators more because of their size, as consequence they need to face with a high number of cyber-attacks. The probability that the organization will successfully defend a network across all attacks falls to nearly zero very quickly. Reporting here the analysis performed by Geer et al, [19] it is possible to imagine for example, three different organizations in an ecosystem in which attackers are at different levels of competencies and skills. It is assumed that Organization A has a 90% probability of successful defence, while Organization B has a 99% probability and the last, Organization C, that has a very high level of defensive infrastructure with a 99.9% probability of successful defence. Each organization has good chances of defending against potential intrusion attempts, considering that Organization A, B and C find dangers in time and defend their networks respectively 90 per cent, 99 per cent, and 99.9 per cent of the time. The issue needs a greater attention when the perspective is transfer to the respective 10 per cent, 1 per cent and 0,1 per cent of the probability in which the organizations are not able to defend their systems. The probability that the organisations considered in the example can successfully defend their network against every intrusion attempt drops to nearly zero very quickly considering a large enough sequence of attacks that big organization are subject to. As reported in Figure 1, Organization A probability to successfully defend its network across the full sequence of attacks drops below 1% by the 44th attack ($90\%^{44}$). Organization B is able to protect the system for longer, but the probability of successful defence drops below 1% by the 459th intrusion attempt ($99\%^{459}$). Organization C has the most robust defensive infrastructure (pointing to the exponential effects of joint probabilities), in fact differently from what occur for Organization A and B, at the 459th attack, Organization C still has a 63.18% probability of successfully defending against the intrusion attempts. In this case the probability to successfully defend its system falls below 1% by the 4,608th attempted attacks ($99.9\%^{4,608}$).

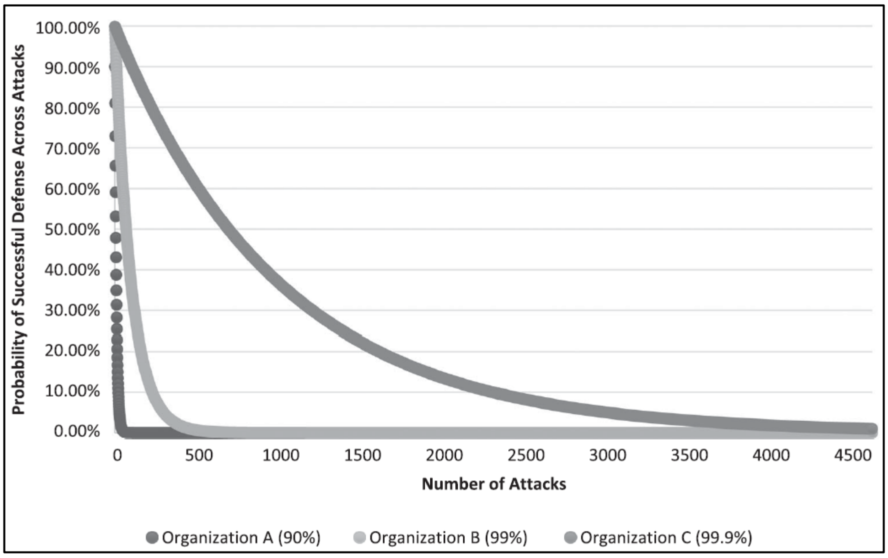

Figure 1 - Repeated attacks and vulnerability of highly targeted organizations (Source: Geer et al, *On market concentration and cybersecurity risk,* Journal of Cyber Policy, 2020, 9)

The defensive performance of Organization C represents a stronger outcome than Organization A and B ones, but considering the Internet context it could be not sufficient. A usually better choice for smaller firms is to be supported by Cloud providers or CDNs in order to improve security performances, but it still depends on the small firm’s probability of successful defence and the intensity of cyber-attacks to the bigger providers. Considering the example reported by Geer et al [19], if a small firm has a 75% of probability to successful defend its system, it would be better off transferring its security provision to the larger providers with 99,9% probability of successful defence in the event they are both attacked once; in this way the small firm will be 24,9 percentage points more secure. But in the case in which the attacks events increase for the bigger firms, the situation becomes more complex. It is possible to understand the circumstances of the example presented here by considering three scenarios depending on the attack-clustering cases reported in Figure 2:

- Scenario 1: the comparative net target value of the big firm is so great that all attacks go towards the concentrated organization, while 0 attacks will be towards the smaller one. In this case the threat component for small firm is equal to 0. In this case the small firm should not transfer the security provision to the larger, since it has 100% probability to not be attacked and to maintain secure its system.
- Scenario 2: smaller organization does get attacked once during the period considered, with a 75% probability of successful defend its system against the attack ($75\%^{1}$). The small organization should transfer the security provision to the bigger one with a probability of successful defence of 99,9% as long as the latter is attacked no more than 287 times, since by the 288th attacks the bigger organization cannot grant more than 75% probability of successful defence ($99{,}9\%^{288}$) that the small firm can have on its own considering the one attack it should be subject to.
- Scenario 3: in this case the smaller organization does get attacked twice during the period considered, leading its total probability of successful defence from 75% to 56,25% ($75\%^{2}$). As a result, the smaller firm has a wider range of security improvements if it transfers its security provision to the bigger one, granting itself a higher probability of successful defence as long as the bigger organization

is attacked no more than 565 times, situation in which the smaller firm should maintain the internal security provision.

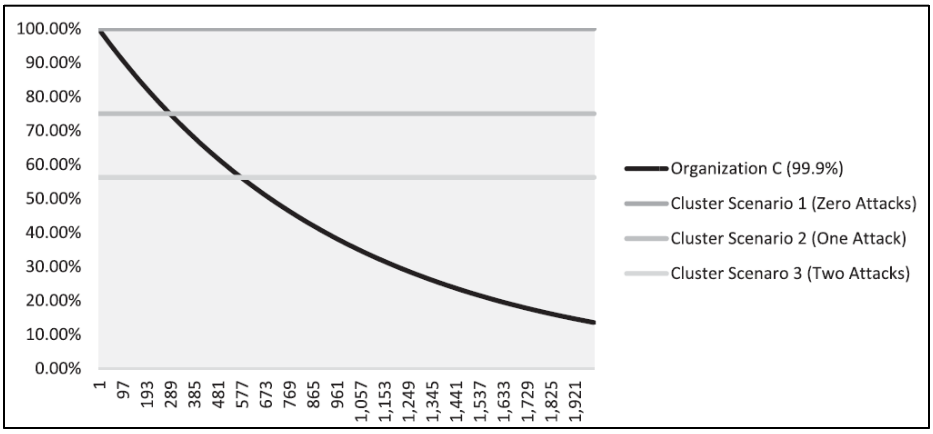

Figure 2 - Outsourcing security in a world of clustered attacks
(Source: Geer et al, *On market concentration and cybersecurity risk,*
Journal of Cyber Policy, 2020, 10)

The analysis sheds light on the security optimization choices that smaller firms need to do and also suggests that the market concentration, by attracting the malicious activities towards these major hubs, can increase cyber risk by producing negative effect on the vulnerability component. Even the bigger and more protected organization, over a large number of attack attempts, has a joint probability of successful defence that asymptotically approaches zero.

3. **Negative effect due to the relation among concentration, scale and complexity**
Market concentration implies that large organization grant a higher level of security by relying on large services and scale. The latter also involves increased complexity, that can occur at two levels: the volume of faulty code and the time it takes to patch flaws. More complexity of code tends to be related to the presence of defective routines potentially exploited by malicious actors. Focusing on the time to patch, it can be defined as "the time it takes for an organisation to correct a certain proportion of vulnerabilities on its systems after the announced discovery of the vulnerability and the issuance of a correction by a vendor" [19]. A faster time to patch is the better choice in order to avoid a too long open window of vulnerability, but organizations need to balance several related benefits and costs. Through the concept of returns to scale, market concentration has a negative effect on remediation velocity as empirically shown by the study performed by Kenna Security and Cyentia Institute [40]. In the study performed, the small firms imply less time to patch vulnerabilities, with respect to medium-large firms, suggesting the harmful effects of concentration

and scale on cyber risk. As explained above, the higher concentration and scale can reflect higher complexity in codes that present more vulnerabilities. The latter need to be patched in a timely manner considering also the higher number of attacks that occur to larger organizations whose time-to-patch is empirically longer with respect to smaller ones.

The third component of cyber risk equation is represented by the ***impact*** that cyber-attacks have on firms and that can be variable. It depends also on market concentration, among other factors. In highly concentrated systems everything is connected, in the sense that what happens in the larger organization has effect on many others. Such interconnections include links among organizations, supply chains and third-party vendors and represent pathways by which the negative consequences of a cyber breach can be transmitted and reach the whole system. From the analysis, it is assumed that concentration negatively affects the impact component of the cyber risk equation.

In sum, the theoretical reasoning that Geer et al. [19] have tried to understand states that the concentration affect cyber risk through the three components: via the threat component there is a redistribution effect, changing who gets targeted by a malicious actor in the first place, given that attackers tend to target the larger centralized organizations due to the potential biggest reward they can allow to perpetrators; via the vulnerability component, market concentration can both reduce individual cyber risk, but also increase systematic vulnerability due to the fact that bigger firms are targeted more than smaller ones leading to lower joint probability to successful defend the system and in addition the longer time-to-patch of larger organizations leaves the users vulnerable for more time; finally, via the impact component concentrated hubs can be characterized by interdependencies that makes arise intensity of impact of a potential cyber breach.

3.2.2. Perceived attractiveness, Internet presence and organizational countermeasures

As understood, the digital economy is driven by consumer information that analysts have called “the new oil” of the 21st century [49]. The related risk is that the availability of data, together with the advances in information technology lead to identity thieves, data breaches and attacks aimed to use information stored. Today, digital activities are easily recorded and stored allowing to collect useful information about vulnerabilities and points of contact. Firms must consequently consider both the benefits from acting online and collecting information, and the risk to be targeted.

Ransbotham and Mitra [50] developed a conceptual model of the Information Security Compromise Process (ISCP) from the perspective of the target organization, that is based on the following three concepts:

1. Attacks are part of a process rather than a single event;
2. ISCP has two paths (deliberate and opportunistic) that have different antecedents and characteristics;
3. Organizational countermeasures play a moderating rather than direct role to deter progression of attacks in each path.

In the construction of this model, they have developed four possible types of attack and 3 constructs that influence the attacks.

Starting from the types of attacks, they developed the following ones: first, nontargeted low-severity attacks are called *information scans* and are used in order to gather information about systems and services, such as a check to see if any machine responds at a particular IP address; second, targeted low-severity attacks, labelled *targeted probes*, test a specific set of potential victims for vulnerabilities; third, nontargeted high-severity attacks, labelled *attack scans*, are widespread, indiscriminate attempts to damage systems, such as a self-replicating worm; finally, targeted high-severity attacks, labelled *targeted attacks*, represent a severe attempt to compromise a specific system.

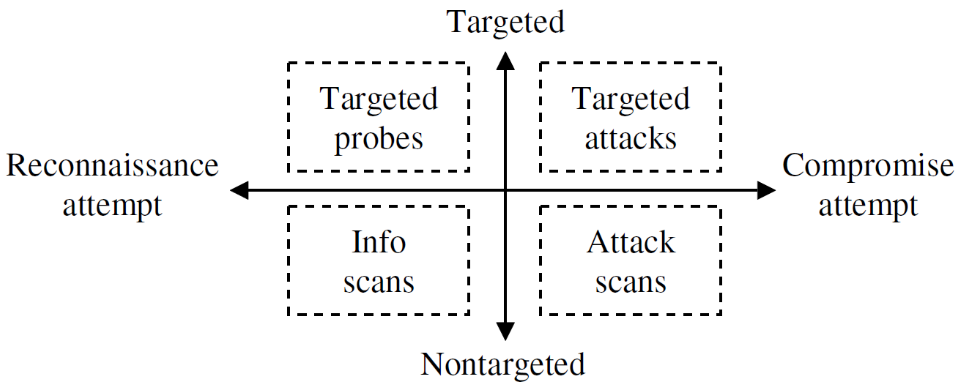

Figure 3 - Attack categories
(Source: Ransbotham and Mitra, *Choice and Chance: A Conceptual Model of Paths to Information Security Compromise,* Information Systems Research, 2009, 7)

Moving to the constructs that influence the incidence of the categories of attacks presented above, Ransbotham and Mitra proposed the following:

- *Internet presence*: size of the firm's internet presence represented by the number of visible IP addresses, number of servers, visitors of the website, open ports, products and number of online ads. Internet presence can be divided in *passive presence* ("number and functionality of the Internet connection of a target firm" [50]) and *active presence* ("volume and types of Internet activities performed by the firm and its stakeholders" [50]);
- *Organizational countermeasures*: efficacy of the countermeasures adopted by an organization that can be represented by the information security practices that has the purpose to reduce risk by finding vulnerabilities and developing policies, procedures, and technology such as patch management, firewalls, intrusion detection systems, and user training that allow them to reduce the threat from cyber-attacks. ISCP model's authors have categorized five dimensions of countermeasures adopted by organizations from the ISO 17799 specifications (Code of Practice for Information Security Management from the International Standards Organization), and security guidelines from the National Institute of Standards and Technology [51], in particular:
  - *Access control:* access restriction by people and software based on need;
  - *Traffic control*: monitoring and identification of inappropriate activities in order to block traffic in case of necessity;
  - *Vulnerability control*: Error removal from hardware/software that can be exploited for inappropriate use;
  - *Feature control*: setting of parameters in software and devices in order to reduce the inappropriate use;
  - *Audit control*: documentation of systems and activities that can be used for audits.

  Traffic and access control measures are used in order to reduce the progression from attack scans and targeted attacks to information security compromise, while vulnerability and feature control is useful in reducing the number of vulnerabilities found through informational scans and targeted probes, reducing the reconnaissance activities. The audit control, instead, improves the other countermeasures by monitoring them and learning.
- *Perceived attractiveness*: overall attractiveness of a target organization based on firm-specific factors, from the perspective of the attackers. The factors that make a target attractive are related to following three dimensions:

- *Tangible value:* valuable information and resources that hackers are motivated to obtain in order to sold to others;
- *Icononic value:* recognition obtained by the attacker in its peer group due to the target's stature;
- *Reprisal value*: satisfaction due to the act of reprisal against an individual or entity.

Focusing on the second concept on which the ISCP model is based, Ransbotham and Mitra [50] have been identified two different paths:

- **Choice: deliberate compromise**
  This first path represents the deliberate attacks on a selected victim, labelled *choice*. In this case the perceived attractiveness construct plays an important role, due to the utility-maximization purpose of criminals. The literature supports the relevance of *tangible value* in the deliberate path, since the effort required to compromise a system have to be commensurate with the perceived potential reward the attacker will gain [52]. In addition, the iconic and reprisal value influences the perpetrator subculture and are an antecedent in the deliberate path. As consequence, "higher perceived attractiveness of the target firm (tangible, iconic and reprisal value) is associated with a larger number of targeted probes" [50].

- **Chance: opportunistic compromise**
  The second path identified represents the opportunistic behaviour of attackers that compromise those systems not previously selected that are more vulnerable to attack. For the identification of vulnerabilities there are a lot of packaged tools, making the related expertise easily available. In this case the degree of Internet presence affects the number of attacks and in particular passive and active presence is more influenced by specific tools used to compromise systems.

  Focusing on passive presence, since it represents the organization's Internet footprint, a larger one has as a result a greater number of nontargeted attacks due to the greater number of information exploited online. This leads to more attacks through the opportunistic path in case of foot-printing and vulnerability-exploitation tools use. The latter are tools that respectively provide information about reachable IP addresses, open ports and service running, and allow the known vulnerabilities exploitation.

Moving instead to active presence, since it refers to the volume and types of online activities, in case of more frequent ones, more information is revealed and can be used to target the system. It leads to more attacks through the opportunistic path in case of use of code-breaking tools (that decipher encrypted transmission and passwords), data-sniffing tools (that allow hacker to analyse transmission content) and system-control tools (that enable hacker to control hosts and sessions).This leads to understand that "a larger active Internet presence of target firm is associated with a larger number of targeted probes" [50].

Despite the distinction made, the two paths can converge and can be used in conjunction. Attackers can identify the systems more vulnerable and then select the ones for specific direct attacks, by making a turn from opportunistic to deliberate compromise. The first concept of the ISCP model is related to this discussion, since it argues that attacks are a process, in fact they can start with initial exploratory attempts that make gain knowledge about the system, and after that a final attempt is used to compromise the system. This makes possible to understand the importance of practices and technology for the protection of systems and data, even if protection can be considered imperfect and can leaves residual risks [53]. It is due to the fact that security technology can often be error-prone, and also that target company may be slow in adopting appropriate countermeasures, showing a time-to-patch not appropriately short to remove the risk of cyber-attacks, as shown above.

The following diagram summarizes the ISCP model analysed.

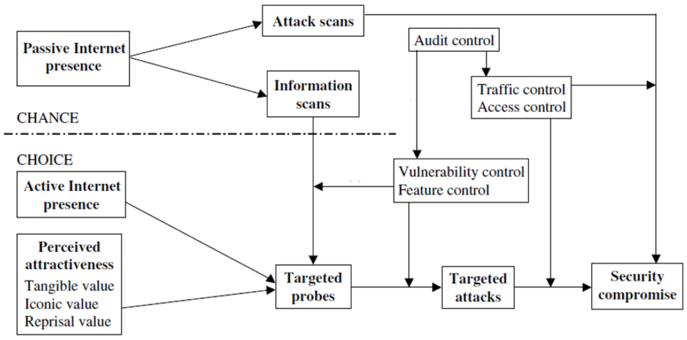

Figure 4 - The ISCP conceptual model
*(*Source: Ransbotham and Mitra, *Choice and Chance: A Conceptual Model of Paths to Information Security Compromise,* Information Systems Research, 2009, 12)

4. Cybersecurity investments

Digital technology has changed the economy, since big data, computing power, cloud-based systems and networked processing have led to the creation of new markets in which organizations can exploit a large range of new opportunities [54]. Data, in particular, have become so fundamental, that a solid infrastructure of data market has been created and strongly exploited. Digital giants such as Facebook, Apple, Amazon, and Google base their business models on traces left by Internet users who visit their online websites. Data brokers also acquire information and gather all sort of information about millions of people both online and offline [61]. For instance, search engines rely on past researches to improve search results, sellers rely on product already bought in the past and online activities to make product recommendations, and social networks make revenues by giving marketers access to their vast user bases [43].

Today, information is easily recorded and stored leading to a reduction in tracking costs. The low cost of collecting digital information lead to the collection of huge amount of data that can be used for learning more about their customers and applying target advertising, price discrimination and customized product recommendations [55]. In this way firms can extract more consumer surplus and increase their profits [61], creating personalized markets, with economic models characterized by asymmetric information and differentiated products. Organizations sell more valuable products through better personalization or quality improvement that are possible thanks to data collection. As result consumers are willing to pay more and it is possible for firms to charge a higher mark-up.

In addition, it is possible to extract a larger share of consumer surplus through personalized pricing, due to the fact that the opportunity cost of providing utility is higher when data are available and can be used for having a better knowledge about customers' willingness to pay. The current websites' ability to dynamically update and personalized prices for each visitor is making the online market closer to the theoretical scenario of first-degree price discrimination [43].

Data also affect the number of targeted ads that a firm decides to show, because well-targeted ads have more value due to the fact they are based on consumers' preferences obtained through information gathering [55].

Using data on a large scale can enable significant increase in revenues as analysed above, but, at the same time, it can also cause adverse implications for market structure, making more difficult to enter in the market for new organizations and implying the development of winnertake-all situations [54]. An additional risk associated with the availability of this huge amount of information is the attractiveness that creates on hackers' perceptions and the potential use they can make of it in case of successful data breaches. In 2006, identity theft has led to $61 billion of corporate and consumer losses, in which the 30% of known identity thefts have been caused by corporate data breaches. In addition, the US Bureau of Justice estimated that in 2016, about 10% of all U.S. residents age 16 or older (26 million persons) reported that they had been victims of identity theft [64].

The data reported show the increased intensity of the phenomenon, the correlated privacy issues that are caused, and the growing trend of companies' involvement in information security. The risk of a cyber-attack, and a subsequent data theft, could affect competing firms' strategies of data acquisition and, in turn, market outcomes (in terms of prices and market entry) since firms can use consumers' data to apply profitable practices, such as explained above. However, previous literature has highlighted how collecting more data can attract the attention of hackers, as the reward for a successful cyber-attack increases [59]. Thus, a firm must balance these two opposite effects when choosing a data acquisition strategy.

In this section it will be firstly reported the different cybersecurity countermeasures that firms can adopt and integrate in their practices and policy, and it will be analysed the field of cyber insurance that has become central in the cybersecurity field, even if it is constantly evolving and is not completely defined yet. After that, there will be a focus on cybersecurity management issue from organizations perspective and, in particular, the boardroom, analysing its involvement with this issue. The cyber countermeasures applied in Italian companies and the cyber-attacks suffered by them will give an idea of the effort actually applied and potentially needed. It will be then investigated the interconnection between the choices taken by firms in terms of cybersecurity investments and the relative effects on market competition, and on the conditions under which the organizations tend to overinvest or underinvest in case of technical and market spillovers effects.

4.1. Governing cybersecurity

The fight against cybercrime is related to both economic and technical issues, leading firms to the development of cybersecurity policy and procedures that try to reach the higher level of confidentiality, integrity and availability of their set of information. In the data-driven economy, dominated by cyber threats, security is a "good" that organizations need to provide to customers in order to maintain their revenue share.

4.1.1. Cybersecurity countermeasures

Information security concerns firms' spending in a variety of areas:

- *Continuous risk assessment*: companies should identify their risk profile by identifying threats and vulnerabilities in order to implement security controls to address these risks;
- *IT environment's health*: companies should ensure that hardware, software and applications such as antivirus software are up-to-date with latest patches installed.
- *Authentication*: the access to company's system and data should be protected with complex authentication means, choosing between at least two among password, devices that generate random PIN and biometric authentication.
- *Internal commitment and responsibility*: since risks are often caused by human errors of companies own staff, a formalised set of policies and procedures ensure a clear way to develop awareness of employees, improving and maintaining system security.
- *Access to information*: companies should ensure that the authorization given to users are restricted and that account of leavers or other third parties that have previously required access to the company's system are timely terminated. Large numbers of controls can address the risk of unauthorized access to companies' data, from manual controls that for example validate periodically users' access rights, to automated controls of automatic mechanisms in the systems.
- *Data retention*: companies should archive and retain data as long as it is required for the business purposes, and after that they should remove them from company's network limiting unauthorized access to sensitive information.
- *Other security controls* such as software used to detect viruses, firewalls, patch management systems, encryption techniques, intrusion detection systems, automated data backup.

By applying all these techniques, firms try to grant security in the different cybersecurity domains (i.e. the areas in which computer systems and network are used), such as the physical, user, application, network and logical domains). Each one has different security challenges to address that are related to hardware and software systems, operating systems, applications, data, user information and how all these aspects are interconnected, accessed and manipulated. It is necessary to determine the cyber risk associated with each domain and implement specific tools and techniques that allow firms to maintain a high level of security protection.

“A security countermeasure refers to a way to detects, prevent, or minimize losses associated with a specific IS threat” [56]. There could be very different countermeasures based on the different threats that have to be addressed. A distinction that could be done is between [56]:

- *Preventive efforts* that include the advanced security software or controls applied to protect the Information Security assets. Examples of this type are firewall, intrusion detection, surveillance mechanisms and the generation of exception reports;
- *Deterrent efforts* that include all the security policies and guidelines developed by organizations, user trainings and education to use Information Security assets in a safety way.

An effective security system should cover and protect the entire IT environment, by defining policy and procedures to follow, educating individuals to operate both online and with IS assets, and to understand the consequences of security systems’ lack. Solms et al. [57] state that the security baseline should consider all the countermeasures for all the assets and threats, but in the real world it is necessary to consider the cost of all the countermeasures to be applied and takes trade-off decisions. The authors divided the IS security into different levels of *Operational Security Environment* (OSE):

- *Ideal OSE*: the highest level of protection without risk to be compromised;
- *Prescribed OSE*: the required level of protection defined by external parties;
- *Survival OSE*: the level of countermeasures that protect the most critical information;
- *Baseline OSE*: the level of protection between the Prescribed and Survival OSE level.

An important factor to be considered in the development process of a high IS network’s protection level is the high probability of errors related to individuals’ actions. The root cause of security breaches can be split in three factors: intended attack by hackers, system vulnerability and the human error [58]. In fact, if a cyber-attack has success, it is only partly due to attackers' competencies and knowledge, but it is also due to the flaws in the system and to the individuals inside the network. Company awareness of the high risk to suffer a data breach due to errors of company's own staff is fundamental in order to put in place a formalised set of policies, procedures and education to the internal resources. In this way the company's staff is more conscious about the behaviours to be taken when they operate online and in the company's network.

4.1.1.1. Cyber insurance

The security countermeasures presented so far are related to *self-protection* tools and techniques that reduce the probability of a security breach, but also *self-insurance* investments can be introduced. The latter mitigate the negative effects caused by the occurrence of a security breach, such as regular backups on existing data, or a cyber-insurance policy.

"Cyber insurance policy is a contract between an insured and an insurer which defines terms, conditions, and exclusions for the insured risk. The insurance premium is a fee paid by the insured to the insurer for assuming the risk." [59]. Cyber insurance is emerging to be an important tool for the protection against losses due to a successful cyber-attack. It is considered as a strategic choice for risk management, since traditional self-protection measures cannot always guarantee an adequate level of protection on specific complex corporate framework [59], and in the case in which they fail in their scope, cyber insurance policies protect the firm against losses occurred. Adopting a cyber insurance policy, organizations choose to share the risk with an external party that better manage the risk on the basis of the evaluations done, in order to support the consequences of a security breach.

Although the growing need of cyber insurances due to the always more threatening cyber space, the current characteristics of cyber insurance market, such as the dominance of large clients, the complex and long underwriting process, tha lack of standardization, and the misalignment between demand and capacity, does not make easy the development of this market.

The difficulties encountered in the application of cyber insurance policies are reported below:

- A first critical point that obstacle the spread of cyber insurances is related to the **lack of standardization**. Cyber insurance can be used for a variety of cyber incidents, such as loss of integrity or availability, data breaches, human errors and, particularly, ransomware. In fact, companies can receive compensation for at least a part of the ransom paid and for losses due to the cyber-attack. However, there could be some areas not so clear in terms of what is covered or not, such as events like errors, omissions, power outages etc., or events to external service providers that have impact on the company, or also corporate entities coverage on different jurisdictions or created during the policy period. The necessity of establish criteria to allow standardization arises and slows down the cyber insurance market development.

- Another critical point related to the difficulty of cyber insurance application is the **underwriting process**. It usually involves long preparatory activities to evaluate and determine risk and all related coverage and exclusion rules. In fact, there is the necessity of a long process related to the information collection that assists in the formulation of the insured risk profile and decide if accept or not the cyber risk. This is because cyber insurance coverage and conditions are not as standardized as other insurance products, also because in this case it is necessary a high level of tailoring based on each company cyber risk profile.
- In addition, there is also the dominant presence of **large companies as customers** in this market, since they are more familiar to cybersecurity issues than smaller firms. The large size of customers adds complexity to an already complicated situation, and leads to longer underwriting process and necessity for customizing policies.
- A significant **imbalance between demand and capacity** does not make the situation simpler. The demand for cyber insurance continues to increase, while the capacity to cover the demand is limited by the difficulties listed above.
- Another critical point is related to the **intercorrelation of cybersecurity risks** since a cyber-attack can affect multiple organizations at the same time and it can occur also in different places. As a result, a single event can incur claims from different insured organizations.

- The **cost** is an obstacle too, in fact insurance contracts tend to be overvalued because of the inability of the insurer to predict losses of the customers, such as the reputational damage.

Cyber insurance is growing a lot despite the difficulties encountered, due to the opportunities that it can bring to firms in the future, but currently it has to face with a lot of challenges prior to standardize and be widely adopted.
The contribution of bug data analytics tools (e.g. data mining, machine learning) are used a lot for security protection. Some impacted areas are for example intrusion detection, malware and ransomware detection, code security. They could also be used for the development of cyber risk prediction models to design insurance products [59].

4.1.2. Cybersecurity from the boardroom

Gale et al. [60] studied, in their 2022 paper, how the Boards of Directors in modern organisations are engaged in cybersecurity with respect to other areas of oversight.
The BoD should develop a cybersecurity plan and the steps necessary for its implementation, but several factors influence these dynamics: the technical nature of cybersecurity, together with the lack of expertise in this field among directors, existing governance structures that have the tendency to leave cybersecurity only to IT departments, and lack of metrics to assess cybersecurity investments.
In addition, employees often omit the "not serious" cyber-attacks and do not report to the BoD the negative results in reports. However, the growth of ransomware attacks and the increasing cybersecurity spending by companies worldwide in the cybersecurity area, lead the BoD to face with the approval of higher budget for this purpose, forcing them to pay attention on the topic. Engagement is too scarce despite the frameworks, standards and guidelines provided (NIST Cybersecurity Framework, NIST SP 800-53, ISO Standards 27001/2/5, COBIT19) [60].

The directors' engagement in cybersecurity is characterized by the phenomenon called *institutional isomorphism*: in case of high uncertainty, organisations tend to imitate practices of comparable organisations and adopt similar structures and processes. The phenomenon is influenced by different types of external pressures:

- *Coercive pressure*: it is characterized by the regulations and industry standards that could also provide the application of significant fines in case of noncompliance. The result, in this case, is that companies are forced to converge towards similar rules and practices. The consequences of this type of pressure manifest in a relatively short term.

- *Normative pressure:* it is determined by professionalisation for which specific work methods are associated with a profession. This is the result of education, trainings, certifications, and experiences that make organisations adhering to specific professional standards and networks. The relative manifestation is over a long-term period.
- *Mimetic pressure:* it is related to the diffusion of practices adopted by certain organisations perceived as role models. In this case information sharing plays an important role. This type of pressure manifests on long-term period.

In addition, *organizational factors* play a role in the directors' engagement in cybersecurity: the lack of managerial and BoD's support lead to a consequent budgetary limitation; past cyber-breaches create more proactivity in responding to additional attacks or to face with cybersecurity issues.

The analysis performed by Gale et al. [60] shows that the lack of confidence of directors on this technical field, that is also characterized by insufficiently formalised reporting practices, make it a topic of low priority for discussions. In addition, boards often delegate cybersecurity responsibility to other entities such as audit, risk committee or IT departments. As consequence, the topic does not receive sufficient attention, and this can result into ill-informed decisions and lack of BoD control on the performance.

The influence of the pressures described above are analysed in the following points:

- The role of coercive pressure is significant and leads to the need for strengthening regulations in this field that should clarify the liability of directors and the top management involvement in cybersecurity.
- The other significant influence is the normative pressure. The directors with a cybersecurity background have more confidence in addressing this topic and this promotes discussion about it in the BoD.
- Mimetic pressure, instead, is resulted to be the one with lower impact on driving directors' involvement with cybersecurity.
- Among the other organizational factors that influence the directors' engagement in this topic, the existence of prior cyber-attacks has a significant role, because

it promotes the discussion in the boardroom. Media reports also have an influence, that could be dual: on the one hand, the presence of reports on recent cyber-attacks could create the basis for an analysis and the relative discussion, but on the other hand it could lead to the optimism bias in cybersecurity, for which directors could consider these events as external that have not hit their companies and are not of their competence.

The analysis reported sheds light on the actual engagement of directors with cybersecurity topics, showing that it is still scares, mainly because of its technical nature and of the sub-optimal cyber-reporting practices.

From the analysis it is possible to imply that ways for the highest involvement of directors in cybersecurity decisions could be the consolidation of reporting practices together with greater communication between BoD and committees to which cybersecurity decisions are delegated. In addition, since the coercive pressure has an important role, regulations should provide clear requirements related to directors' responsibilities for cybersecurity oversight. Trainings in cybersecurity and creation of related certifications could be an option to increase the professionalisation of directors, making them more confident in addressing the topic.

In March 2022, the Securities and Exchange Commission (SEC) proposed legislation in which the boards are obliged to include cybersecurity experts among directors.

4.1.3. Italian cybersecurity measures' adoption

The security measures are necessary for at least minimize the cyber risk, even if also the best security practices can be bypassed by the higher skills and expertise of perpetrators. The situation documented in Italy by the 2017 Bank of Italy report is presented here as example of the power of cyber-attacks even in presence of security measures [1].

The data reported by the Bank of Italy are from surveys that have been carried out on Italian private business sector, with relation to industrial and non-financial service firms, for the period September 2015 – September 2016. The relative results are statistically representative for macro-region, size, technological intensity and share of exports. The results about the cybersecurity management in Italy, based on the categories described, are reported in the table below:

	Internal resources	*Outsourcing within group*	*Outsourcing outside group*	*Internal + Outsourcing*	*No cybersecurity*	*Don't know / No answer*
Geographical area						
North-West	35,2	5,0	27,2	29,1	0,7	2,8
North-East	30,0	6,9	28,3	31,1	1,9	1,8
Centre	42,8	6,1	22,9	22,7	2,2	3,2
South and Islands	46,8	4,1	24,1	20,1	2,0	3,0
Number of employees						
20 – 49	35,4	4,6	30,6	24,5	1,7	3,1
50 – 199	39,6	7,6	19,7	30,2	1,5	1,4
200 – 499	46,6	5,4	7,8	37,7	-	2,5
500 and over	42,9	10,4	5,1	36,9	0,1	4,7
Tech/knowledge intensity of sector						
High & medium-high	43,4	5,8	19,4	27,3	0,5	3,6
Low & medium-low	34,9	5,5	28,7	26,7	1,9	2,3
Exports as share of turnover						
Less than 1/3	38,2	5,5	27,0	25,0	1,8	2,6
Between 1/3 and 2/3	33,2	5,5	27,0	31,4	0,3	2,6
Over 2/3	37,2	5,8	20,6	31,7	1,8	3,0

Total	**37,2**	**5,6**	**26,2**	**26,9**	**1,5**	**2,6**

Table 1 – Cybersecurity management in Italy

It is possible to understand from data that the major part of cybersecurity measures are developed internally, in fact the 37,2% of firms fall into this result, but it is interesting to notice that in Southern Italy there is the greater tendence to adopt cybersecurity measures by using internal resources (46,8 % of firms in the south of Italy and in the islands), maybe because in this area there could be limited availability of high-tech firms that provide this type of services, with respect to the rest of the country. In the Northern area, especially in North-East of Italy, there is preference for outsourced services' adoption in order to make systems safe.

Surveys' evidence based on the size of the firms shows that larger firms are more likely to internally manage the cyber risk and only partially outsource it to external providers (Only 5,1% of larger firms totally outsource the cybersecurity management, while the major part of them have internal resources for this purpose or combine both internal and external resources). This is probably because greater firms are the ones that manage greater amount of data, and so the primary targets for attack (in fact, the percentage of them that do not adopt cybersecurity measures at all are close to 0%). In this perspective, it is safer for them not to give too much control on data and infrastructures protection to external that could be used for supply chain attacks.

In addition, it is important to know that for smaller, low-tech firms, external providers primarily are retail computer sellers, while the internal resources engaged on data and system protection are not cyber experts, but only the ones with higher IT skills than other ones in the company; as consequence, cybersecurity is not handled by professionals. On the other hand, the external providers to which larger firms outsource cybersecurity are specialized firms, while internal teams are at least partly represented by cybersecurity experts.

High and medium-high tech firms are probably the ones with more internal expertise, and this leads them to rely on their resources, with a 43,4% of them that manage cybersecurity internally.

Looking now at the firms that export abroad, the firms whose turnover from exports exceeds the 2/3, are more likely to be represented by the larger firms in terms of number of employees, in fact it is possible to notice similar results for them, so a greater reliance on internal resources or partially combined with external ones, in order to maintain greater control on the large amount of managed data.

	Cybersecurity measures' adoption	**No cybersecurity**	**Don't know / No answerr**
Geographical area			
North-West	96,5	0,7	2,8
North-East	96,3	1,9	1,8
Centre	94,5	2,2	3,2
South and Islands	95,1	2,0	3,0
Number of employees			
20 – 49	95,1	1,7	3,1
50 – 199	97,1	1,5	1,4
200 – 499	97.5	-	2,5
500 and over	95,3	0.1	4,7
Tech/knowledge intensity of sector			
High and medium-low	95,9	0,5	3,6
Low and medium-low	95,8	1,9	2,3
Exports as share of turnover			

Less than 1/3	95,7	1,8	2,6
Between 1/3 and 2/3	97,1	0.3	2,6
Over 2/3	95,3	1.8	3,0

Table 2 – Aggregated value of cybersecurity management in Italy

Aggregating the fields related to *cybersecurity measures' adoption* (*Internal resources, Outsourcing within group, Outsourcing outside group, Internal + outsourcing*), it is possible to have a better overview about the awareness on cybersecurity, translated in the application of cybersecurity measures, even if it is important to know that there is no information about the type of security measures, and so, on their quality and effectiveness. Considering the part of no respondents, which represent an average 2,6%, the remaining part is characterized as follow: almost the totality of firms in all areas is aware of the cyber risk and applies measures to increase security. This is particularly true for the Northern area of Italy, the firms with 50-199 and 200-499 employees, high and medium-high tech firms (even if low and medium-low tech firms present only a slightly lower percentage), and the companies whose share of turnover from exports is between 1/3 and 2/3.

Turning to the cyber-attacks against the firms in Italy, the relative Bank of Italy survey's results are reported below:

	No attack	***At least one attack***	***Don't know / No answer***
Geographical area			
North-West	62,1	28,5	9,4
North-East	56,9	32,5	10,6
Centre	53,8	35,3	10,9
South and Islands	70,0	24,4	5,6
Number of employees			
20 – 49	63,2	29,2	7,6
50 – 199	57,6	31,3	11,1
200 – 499	45,4	36,7	17,9
500 and over	39,3	34,8	25,9
Tech/knowledge intensity of sector			
High & medium-high	57,3	30,5	12,1
Low & medium-low	61,6	30,1	8,3
Exports as share of turnover			
Less than 1/3	62,5	29,4	8,1
Between 1/3 and 2/3	54,3	34,6	11,1
Over 2/3	57,1	29,0	14,0

Total	**60,4**	**30,2**	**9,4**

Table 3 – Cyber-attacks against Italian non-financial firms

It is possible to understand that the probability of being attacked at least once is higher when firm size increases. In fact, larger firms are more attractive since they handle more data and probably more valuable ones**.** An additional factor that explains this result is that they are more exposed, better known, and their dependence on the network is higher since they have more employees that use more devices connected to the Internet and can also engage in risky behaviour. These firms need wider networks and are in the supply chain with a high number of external suppliers that may have access to IT assets of the firm. Survey's results show that exposure probably plays a role, in fact firms that export between 1/3 and 2/3 of their products or services are more likely to be attacked. In fact, attackers can operate all over the world and are not limited by boarders: firms that exchange information abroad and have a market in foreign countries have more probability to become targets compared to others which operate in their state, make lower use of Internet communications and are less known on a larger scale. This should apply even more to firms that export more since their trend should be in line with the one of larger firms that are better known on a larger scale, but in this case the results could be affected by the non-respondents that are a high percentage for this group. Firms located in South Italy show less probability to be attacked and this is maybe due to the fact that in this area firms tend to have lower technology use and are less visible to hackers and less interesting. On average, one third of firms in Italy reported to have been subject to at least one attack that has caused damages.

The author of Bank of Italy report, Claudia Biancotti, estimates that a portion of the respondents of the survey did not disclose the real information about cyber-attacks suffered. Indeed, the literature suggests that in these cases there could be present two sources of bias: the imperfect knowledge of the phenomenon due to lack of technical knowledge, and the reticence to disclose attacks since it potentially leads to reputational damages, regulatory fines, legal fees, loss of business. As consequence, the author corrected the model in order to address the non-responses. The results from the corrected model show that the share of firms hit by at least one attack goes up, until 45,2%.

The study conducted by the Bank of Italy sheds light on the fact that it is necessary a greater effort in the investments. As company grows, cybersecurity becomes less easy to manage and more investment is needed. Cybersecurity investment, indeed, are necessary in order to manage the cyber risks with the best solutions and to the highest possible extent. In the following section it will be presented the optimal level of investments that firms should adopt in order to minimize risk.

4.2. Cyber investments and competition

The fight against cybercrime can be considered both from an economic and a technical perspective, in which attackers and defenders respond to incentives [61]. Security can be seen as a “good" and it is the result of the choices of various actors in the system [62]. In the analysis performed by De Cornière and Taylor [62], it is presented how firms' incentives to invest in cybersecurity are influenced by the competitive environment in which they operate. The authors study a model of competition for firms that offer differentiated product and that have to face with attackers who want to steal information by exploiting vulnerabilities on their IT systems. A key characteristic of the model is the presence of *negative network effect*, due to the fact that customers will be hurt in case of attacks to larger firms, the ones more attacked due to the amount of information they handle [19]. The model that will be reported in this section focuses on how much the firms decide to invest to eliminate vulnerabilities in order to prevent breaches.

Prior to present the model, the **competitive environment** is assumed to be characterized by three parameters [62]:

- *Intensity of competition*, measured by market structure (in this case there is a comparison between monopoly and duopoly) and the degree of substitutability of products;
- *Consumers' awareness of security risk*, measured by the extreme situations: most of the costumers are naïve about security and most costumers are quite savvy;
- *Firms' business model*, distinguishing between *pricing regime*, in which firms sell a product and have to choose the relative price *p* (e.g. cloud service providers), and *advertising regime*, in which firms monetize users in different ways (products are free) and try to maximize demand consequently (e.g. advertising-supported platforms); *R* represents the expected per-user advertising revenue.

The **security** level of the firm's IT system is related to the vulnerabilities that hackers will try to exploit and, at the same time, that firms try to find and fix in order to reduce the probability that an attack will be successful. This probability is denoted by 1- σ_i, where σ_i is firm *i*'s level of protection (or the share of vulnerabilities that are fixed). Fixing vulnerabilities requires investments in security with the relative costs related to the hiring of software engineers for vulnerabilities in the code or to patch exposed ones, or to the training of employees against phishing that amounts $\frac{k\sigma_i^2}{2}$. Hackers observe the level of protection of each firm that they can potentially target and decide on who launch the attack, incurring in a cost *c*, represented by the required effort and the risk to be caught. The hacker's expected payoff per customer is h. From the firm perspective, instead, a successful breach causes a damage Δ represented by the administrative cost of responding and the IT costs for any damage caused, reputational damages, or even a fine imposed by regulators. As consequence of a cyberbreach, the firm *i*'s payoff is

$$\pi_i = [r_i - h(1-\sigma_i)^2\Delta]n_i - \frac{k\sigma_i^2}{2}$$

Where r_i represents firm *i*'s per-consumer revenue (r_i=p_i in the pricing regime and r_i =*R* in the advertising regime), the term $h(1-\sigma_i)^2\Delta$ represents a marginal cost because the breach probability depends on the firm's demand and it has to be subtracted to the marginal revenue of the firm in order to find the marginal payoff. The latter is multiplied for the number of customers of firm *i* (n_i) and then decreased by the cost needed to fix vulnerabilities in the system ($\frac{k\sigma_i^2}{2}$).

The model assumes that the cyber-attacks exploit the zero-day vulnerabilities presented in Chapter 2. Systems in which there are greater number of users are more attractive for hackers, since they can potentially compromise all system's users, and in case of a successful attack, the damage for customers is denoted by *L*.

As a first benchmark, the authors computed the optimal efficient level of investment in order to maximise the total welfare, excluding hackers' payoffs both in case of duopoly and monopoly. In the former case, having $\sigma_1 = \sigma_2 \equiv \sigma$ the efficient investment level is:

$$\sigma_\omega^* = \frac{h(L+2\Delta)}{2k+hL+2h\Delta}$$

The efficient investment level is increasing with respect to *h* (hackers' payoffs), *L* (damage for customers) and Δ (damage for firms), while it is decreasing with respect to *k* (cost of providing security).

Analogous result in the monopoly framework, in which the efficient investment level is:

$$\sigma_{\omega}^{*} = \frac{2h(L+\Delta)}{k+2hL+2h\Delta}$$

The relationships seen for the duopoly case are maintained.

The **monopoly case** in both pricing and advertising regime is presented below.

- **Pricing regime**

  The monopolist has to set the price and has two available strategies to follow: serving the whole market, both savvy and naïve consumers, or serving only naïve consumers. Savvy consumers, that represents a share μ of the total customers n, are more sensitive to the security profile of the firm and have a willingness to pay that is reduced by the security risk they perceived in the firm's IT system ($V - hL(1-\sigma)^2$), where V represents the value they evaluate the product. Naïve customers, instead, are less sensitive to security risk, and their willingness to pay is not affected by the security risk issue.

  In the case in which the monopolist decides to serve all the market, he can apply a price that is equal to the willingness to pay of savvy customers, lower than the naïve customers' willingness to pay. This can be done through the implementation of the efficient level of investment in order to improve the perception that savvy customers have about the security risk level of firm's IT system; in this case the firm fully internalizes consumers losses.

  Alternatively, the monopolist can serve only naïve consumers, which don't respond to security investment. For this reason, monopolist has no incentives to invest in security. In this case the firm does not internalize the consumers' losses and provide a security level under the efficient one. The result is an underinvestment from a social perspective.

- **Advertising regime**

  In the advertising regime, it is impossible for the monopolist to extract the level of security from customers, having no price to set, and therefore he cannot internalize consumers' losses. In this case the firm invests less than the efficient level.

The **duopoly case** is now presented below, also in this case focusing on both pricing and advertising regimes.

- **Pricing regime**

In the pricing regime of a duopoly, the two firms have to choose a price in order to maximize their profit, taking into account the different types of customers and the relative demand function: sophisticated consumers observe the security level of the firms' IT systems and for this reason their demand is characterized by a *negative network effect* for which, if more consumers choose firm i, the probability that it becomes a target increases, and the sophisticated consumers will consider less attractive firm i; naïve consumers, instead, do not observe the security risk of the firms in the duopoly.

The investment in security has a price *competition-intensifying strategic effect* that operates through two channels:

- *cost channels*: in this case if firm *i* invests in cybersecurity, it faces a lower effective marginal cost, indeed, anytime an extra consumer chooses firm i, the expected damage increases of an amount which is decreasing in σ_i $((1-\sigma_i)^2\Delta)$. In other words, for each new consumer that chooses firm *i*, the expected damage increases (due to fact that firms with more customers are the most targeted), but of an amount that decreases if the firm makes more security investment, leading to a lower marginal cost. The reduction in the effective marginal cost leads firm *i* to reduce prices and, for strategic complementarity, also firm *j* will reduce them.
- *demand channel:* if firm *j* increases its level of protection σ_j, its attractiveness increases and consequently firm *i*'s demand decreases. In addition, firm *i*'s sensitivity increases (its demand becomes more price-elastic) due to the reduction in the *negative network effect* that now affects grater firm *j* that is acquiring more market share with the highest investment done in security. Due to the greater price elasticity, firm *i* has incentive to lower prices in order to increase demand. By strategic complementarity, firm *j* reduces price too. As result, the investment in security leads to the reduction of the *negative network effect* strength, intensifying the price competition.

The consequent equilibrium level of investment is:

$$\sigma_p^* = \frac{h(4\Delta - L\mu)}{6K + h)4\Delta - L\mu)}$$

It is possible to analyze the relationship between the firm's equilibrium investment level in security σ_p^* and the parameters L (damage for customers in case of security breach) and μ (share of savvy customers): the equilibrium investment is decreasing with respect to the share of sophisticated customers and to the damages for customers in case of successful attacks. This means that when the share of sophisticated users is higher and when the damages for customers increase, firms don't have incentives to invest more in security, because of the *competition-intensifying strategic effect* explained above.

The authors also report their analysis on the relationship between μ and L, and the equilibrium price p^*: they have a positive relationship since μ and L amplify the *negative network effect* and make firms less willing to cut prices to attract new customers. Focusing in particular on the share of savvy customers in the market, an increase of μ causes the rival firm to increase investments and increase prices (softer competition) and in this way firms' profit increase as more consumers become savvy.

The cost of security k also has a positive relationship with p^*, since less security (due to the higher cost of providing it) leads to stronger *negative network effects*, and as consequence firms has less incentives to reduce prices.

For what concern the parameter h that represents the hackers' gains, the authors reported an inverted-U shaped relationship with the equilibrium price p^* due to two opposite effects: on the one hand, an increase in hackers' payoff induces firms to invest more in security, attracting more customers and consequently intensifying competition that leads to price reduction; on the other hand, higher value of h amplifies the *negative network effects* that soften competition, leading to higher prices. The second effect prevails in the case in which the cost of providing security k increases, and as consequence, the firms' incentives to reduce prices decrease.

From the analysis made just above, it is possible to state that transferring from a monopolistic market structure to a duopoly, the investments in security reduce due to the fact that, differently for what happens in monopoly, in case of duopoly in pricing regime, prices are a decreasing function of the level of security. On the other hand, starting from duopoly, an additional firm can mitigate the *competition-intensifying strategic effect* because in case of many competitors, a change in only one firm's investment, has a small impact on rivals' pricing. As result, the number of competitors has a non-monotonic effect on investment in case of pricing regime.

- **Advertising regime**

In the advertising regime no price has to be chosen and the model delivers different predictions in the case of ad-funded firms.

Firstly, there is a positive relationship between L and μ, and security investments, since if consumers are more sensitive to security issues (increase in the share of savvy customer that are more attentive in the damage they can suffer from a breach in the firm's IT system), firms invest more in security, in order to increase demand.

Second, in this case there could be over-investment with respect to the social planner's equilibrium because of the *business-stealing effect* for which if R or μ are higher, the private payoffs in case of larger security investment are better than the social one. This results in over-investments in security by firms. The aspect to notice is that the ad-funded business model is characterized by B2C markets, where customers are more likely to be as naïve ones, leading to lower value of μ. As consequence, the over-investment will arise in the case in which there is little product differentiation.

Third, investments are higher than the one of the monopolistic case because of the intent to avoid losing savvy customers to a rival. In this case competition leads to more investments in security.

4.3. Cyber investments and social welfare

Fedele et al. [63] developed an analysis in order to focus on the conditions under which the organizations tend to overinvest or underinvest with respect to the social efficient level of investment in cybersecurity measures. The theoretical literature related to firm decision to invest in cybersecurity has evolved over time even if it is an early stage yet. Until now, four streams of literature, that represent the basis of the analysis, can be distinguished:

1. Gordon and Loeb (2002) [64] investigated the firms' incentives to invest in cybersecurity referring to the framework of one firm only. The results of this analysis are not of general applicability from a policy perspective due to the fact that in the

real world firms almost always operate on common networks and/or are competitors in the product market;

2. Kunreuther and Heal (2003) [65] and Varian (2004) [66] used multi-firm framework in order to investigate the interdependent security. They particularly focus on firms' investments decisions that operate on a common computer network, but that are not competitors in the product market. An example for this case is the cyber breach occurred in 2013 having Target Corp. and Fazio Mechanical Services Inc. as victims. The latter were interconnected due to business necessities and Fazio company was used by attackers in order to access the Target Corp.'s IT systems;
3. Garcia and Horowitz (2007) [67] focused on investment decisions of firms that are competitors but that not share the same computer network. An example to report in this case is that of Amazon and eBay that are competitors in the e-commerce sector, but that use different computer systems for business activities.
4. A more recent literature investigates the investments of firms that are both competitors and use the same computer network. The banking sector represents an example in this case, because banks are competitors but that rely on the same computer systems, such as SWIFT (Society for Worldwide Interbank Financial Telecommunications) network.

To provide a comprehensive framework, five dimensions that characterize the literature developed are reported below:

- *Investment*

  It refers to the two different scenarios that can arise: *continuous investment* in which cybersecurity investment level can take any nonnegative value in the set of real numbers, and *dichotomous investment*, in which there is a simple decision related to invest or not (binary decision).
- *Interdependence*

  It refers to the two cases in which there is only one firm (one-firm settings) using decision theory, and in which there is a panel of firms (multi-firm settings) using a noncooperative game theory.
- *Welfare*

  It indicates, in case of interdependences, the socially efficient investment level that is compared with the equilibrium level.

- *Spillovers*

  This dimension is related to the different forms of externalities that could occur in the multi-firm settings:

  - *Technical spillovers*: in this case firms are not competitors but are interconnected through a common computer network; when a firm invests in cybersecurity, there is a positive externality for which the probability of a security breach suffered by all the other firms on the network is reduced.
  - *Market spillovers*: in this case firms are competitors, but use different computer networks, when a firm suffers a cyberattack, it is assumed to lose clients who shift to competitors.
  - *Market and technical spillovers simultaneously*: in this case firms are both competitors and interconnected by using the same computer network; the externalities seen just above coexist.

- *Network*

  In those cases in which there are technical spillovers, there are two types of computer networks that connect the firms: *exogenous network*, for which the topology of the network is exogenously assumed; *endogenous network*, for which the topology of the network endogenously arises as solution of an optimization problem.

The model of investment in cybersecurity built by Fedele et al [63] reported below is structured in two main section: one-firm setting in which it is analysed the no interdependencies framework, and then multi-firm settings with interdependencies by analysing the different cases of technical spillovers, market spillovers and finally both of them. In all cases, a comparison between investment equilibrium level and the socially efficient investment level (the level of investment that maximises the sum of all firms' payoffs) is made in order to understand the condition under which the firms decide to under- or over-invest with respect to the social investment.

- **No interdependence**

  In this case it is presented the simplest framework, with a one-period model with only a one decision maker with no interdependencies, hence with no factors pertaining to other agents that influence the decision process. The optimal investment level is denoted by I^* and represents the level at which the marginal benefit of the investment (i.e. the reduction in the expected loss due to a cyberattack) is equal to the marginal cost. In this case it is:

$$I^* = \sqrt{vaX} - 1$$

where, $v \in [0,1]$ is the vulnerability of the firm information set, that is the probability of an information set security breach before any investment in cybersecurity is made; $a \in [0,1]$ is the monetary loss due to a security breach; X is the value of the firm information set, referred to as the firm revenue. The insights that can be deducted from this result are that there is a positive relationship between I^* and both the loss incurred by the information set to be defended (aX) and the system vulnerability v.

In addition, by dividing the optimal level of investment by the expected loss without protection, it can be found that the maximum value of I^* is 0,25 of vaX; in other words, the optimal investment level is never higher that 25% of the expected loss before the firm has made any security investment. As consequence, it can be deducted that the value of the expected loss without investment in cybersecurity is always higher than the investment itself, leading to the idea that is better considering investing. The just calculated upper bound for the investment level is instead 36,8% for Gordon and Loeb [64]. For others, like Willemson [68], the upper bound does not exist, since the cyberattacks can be totally neutralized by investing enough money.

The issue is not simply to choose whether to invest, but also when invest. In fact, cybersecurity investments are characterized by irreversibility because it is very costly to disinvest when the investment is already done, and it is hard to manage the enduring uncertainty about the occurrence of a breach. Both the irreversibility and the uncertainty can lead firms to the decision of deferring the investment. The firm will invest now in the case in which the net present value of the investment is positive and also higher than the option value of deferring until uncertainty is reduced, as in the case a security breach occurs.

In addition to the *security risk* that the firm considers by making an investment in security, a risk-adverse firm could also consider the *investment risk*: countermeasures might not work as they should have done. It can increase and exceed the security risk. The investment decision is then affected by the trade-off between the two types of risks.

- **Technical spillovers**

  In this case it is considered that a firm information set is completely vulnerable (v=1) when no security spending has been done. In this multi-firm setting, the technical spillovers occur when firms operate on a common computer network but are not competitors in the product market. The investment made by one firm makes the probability of a security breach reduced for all the firms within the network (*technical spillovers effect*). Considering this form of interdependence among firms that use the same network changes the outcome compared to one-firm framework, in fact the optimal investment level in case of N=2 is:

$$I_T^*(2) = \frac{\sqrt{aX} - 1}{1 + e}$$

where parameter $e \in [0,1]$ represents the positive spillovers produced by the firm i ($\neq j$) investment on security of the network, enjoyed also by firm j. When e=0, it means that no technical spillovers occur, since an investment in security of one firm does not create any benefits in term of security to the other firms; when e=1, technical spillovers occur at their maximum, since the probability reduction of a security breach due to the investment done by one firm in the network, is equal to the probability of all other firms. Looking at the investment level in case of two firms, it is possible to understand that if e>0 increases (higher *technical spillover effect*), the equilibrium level of investment $I_T^*(2)$ is increasingly lower than the one calculated in case of one-firm setting I^*.

$$I_T^*(2) < I^*$$

$$\text{if } e>0$$

The reason behind that trend is that the growing positive effect of technical spillovers yields to *free-riding* behaviours, for which each firm increasingly free rides on the other firms' investment effort. When instead e=0, $I_T^*(2)$ is equal to the equilibrium investment level in the case of one-firm framework I^*, given that no spillovers effect enables free-riding behaviours.

$$I_T^*(2) = I^*$$

$$\text{if } e=0$$

If the equilibrium investment level in case of technical spillovers is extended to N firms, it is equal to:

$$I_T^*(N) = \frac{\sqrt{aX} - 1}{1 + (N-1)e}$$

Also in this case, if *e*=0, the equilibrium investment level equals the one of one-firm setting, but it is increasing lower if *e*>0 rises, due to the free-riding behaviours of the firms that have not invested in security.

In the case computer networks connect an increasing number of firms, this lead to a reduction in the per-firm investment in security due to the free-riding. This phenomenon gets worse when each firm can free rides on a growing number of firms' investments within the network. In other words, the equilibrium investment level shrinks when moving from monopoly to duopoly.

Now, it is possible to compare the equilibrium investment level with the socially efficient investment. The latter represents the investment level that maximize the sum of all firms' payoffs and, in case of technical spillovers, is:

$$I_T^E(N) = \frac{\sqrt{[1 + (N-1)e]aX} - 1}{a + (N-1)e}$$

By making a comparison between the equilibrium investment level $I_T^*(N)$ and the socially efficient investment level $I_T^E(N)$, it can be seen that the former is lower than the latter.

$$I_T^*(2) < I_T^E(2)$$

This means that in case of technical spillovers, firms tend to underinvest with respect to the social efficient level. Fedele et al [63] argue that the underinvestment is due to the *technical spillovers effect* that creates a positive externality, indeed when firm *i* decides to invest I_i in security, its marginal benefits (the increase in its payoff) is lower than the social marginal benefit (the sum of all firms' payoffs). This is because the private marginal benefit does not internalize the reduction in probability of a security breach enjoyed by all the other firms.

Kunreuther and Heal [65] also analysed the conditions under which firms invest in case of technical spillovers, but focusing on the choice to invest or not in cybersecurity instead of how much invest. In their analysis they found that the Nash equilibrium of the game in which two firms decide if invest or not I_i= [0,1] is:

$$R_T(I, I) - R_T(0, I) \geq I$$

The left side of the equation above represents the benefit in case both firms invest instead of only one does it (i.e. the benefit due to the reduced probability of a breach). It is higher than the investment cost and it means that the revenue for a firm i when also firm j invests in security is greater.

Considering for a moment a one-firm setting, the authors show that its willingness to invest is related to the following condition:

$$R_T(I,0) - R_T(0,0) \geq I$$

The condition reported above means that the firm will invest only if it is find profitable to do it (the benefit due to the reduced probability of security breach is higher than the investment cost).

By comparing the two left sides of the equations reported above, the authors find that, when *e*>0 (i.e. technical spillovers increase) the following relationship occurs:

$$R_T(I,I) - R_T(0,I) < R_T(I,0) - R_T(0,0)$$

It means that the benefits from the investment in security in the case in which technical spillovers occur are less with respect to the case of one-firm setting. As consequence, it is possible to understand that the investment decision in the first case is less effective due to the free-riding behaviours (reduced incentive to invest in cybersecurity for the firms that free ride on the other firms' investments). As result, it is possible to say that it has been found that the presence of a second firm that operates in the same network reduces the incentive for investments in security. When the number of firms in the same computer network (*N*) tends to ∞, the per-firm investment in security tends to *0* [63], [65].

Making a comparison with the socially efficient investment level in case of technical spillovers, it is possible to conclude that underinvestment occurs.

Also Lelarge and Bolot [69] find a similar results that corroborate the theoretical findings so far reported. They consider also an indirect *risk of contagion* from other firms attacked in the same computer network. They found that even if an investment erases this indirect risk, underinvestment arises. The idea behind is that in a framework in which an increasing number of firms that operate in the same computer network decide to invest in order to reduce the direct risk of a security breach, there is a reduction of this direct risk for any single firm because the probability that attacks occur in a network where viruses spread (risk of contagion) less easily is very low. The result is the reduction of the incentive for any single firm to invest.

Grossklags et al [70] extended the analysis by considering different types of cybersecurity: the type of countermeasure considered so far is related to *self-protection* investments that reduce the probability of a security breach, but it can be introduced also the *self-insurance* investments, that mitigate the negative effects caused by the occurrence of a security breach, such as regular backups on existing data, or a cyber-insurance policy. The authors have found that the self-protection investments can be suboptimal in terms of social welfare perspective, while the self-insurance investments are at the socially efficient level. This analysis makes it clear that different types of countermeasures against cyber risks differently affect the incentive to invest in cybersecurity of firms.

So far, it has been understood that the technical spillovers effect leads to positive externalities described above (i.e. in case of investment in security of a firm, all firms that operate on the same computer network enjoy the reduction in probability of a security breach), that in turn lead to underinvestment with respect to the social efficient level due to free-riding behaviours.

- **Market spillovers**

  As set in the case of technical spillovers, it is considered that a firm information set is completely vulnerable (*v*=1). In this multi-firm setting, firms are competitors that operate on different and non-interconnected computer systems. As consequence, differently from what occurred in case of technical spillovers, the investment in cybersecurity made by each firm does not implies a benefit in terms of reduction in cyber risk for competitors (i.e. no technical spillovers effect occurs). At the same time, when a firm suffers a cyber-attack, it is supposed that consumers shift to the competitor (i.e. the entire revenue share is lost for the firm that has been attacked) (*market spillovers effect*).

  Fedele et al [63] reported also in this case the optimal equilibrium investment level under duopoly, that is:

$$I_M^*(2) = \frac{X + 6H^2}{6H} - 1$$

where *X* denotes the market revenue that is considered to be equally shared among competing firms, while *H* represents an explicit function of *X*. By comparing the investment equilibrium level ($I_M^*(2)$) and the equilibrium level in case on no interdependence seen above (I^*) it is possible to see that the former is lower than the latter for any given *X*>1.

$$I_M^*(2) < I^*$$

This means that moving from monopoly to duopoly the equilibrium investment decreases, as happened in case of technical spillovers even if the mechanisms behind this tendency are different. In fact, a monopolistic firm that invests in security, reduces the probability to be victim of a cyber-attack and it gets the entire market revenue *X*, while in the case of duopoly under market spillovers, the investment done by a firm is less effective, because it gets the entire market revenue *X* (as in the case of the monopolistic firm) only if the competitor suffers a security breach, whose probability is lower than 1 for any positive investment done by the other firm [63]. By analysing the findings by a welfare perspective, it is necessary first to compute the socially efficient investment level, that is:

$$I_M^E(2) = \sqrt[3]{X} - 1$$

By comparing the optimal investment level $I_M^*(2)$ and the socially efficient investment level with *N*=2 $I_M^E(2)$, it is possible to see that the former is higher than the latter for any given *X*>1.

$$I_M^*(2) > I_M^E(2)$$

This means that the firm invest too much with respect to the socially efficient level of investment. This result is due to negative externalities originated by the market spillovers, in fact if firm *i* invests I_i in security, the benefit due to the investment done are enjoyed only by the firm *i* (i.e. there is an increase in firm *i*'s payoff) and not by the firm *j* (i.e. firm j does not benefit of the reduced probability of a security breach, due to the *market spillover effect*, and firm *j*'s payoff does not increase consequently). This means that the private marginal benefit is higher than the social marginal benefit, because the former does not internalize firm *j*'s reduced opportunity to have the share of revenue of firm *i*. The figure 5 reported below plots the different investment levels in security: $I_M^*(2)$ (red curve), I^* with a=1 (black curve) and $I_M^E(2)$ (green curve).

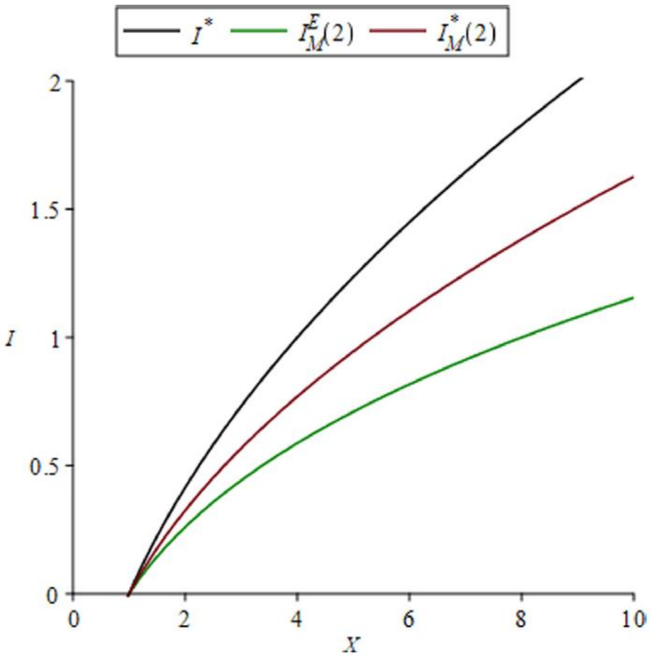

Figure 5 - Equilibrium and socially efficient investments with market spillovers
(Source: Fedele et al, *Dangerous games: A literature review on cybersecurity investments,* Journal of Economic Survey, 2022, 16)

As explained above and as it can be possible to see in the graph reported here, the optimal equilibrium investment is lower than the investment level in case of monopoly, but higher than the socially efficient level of investment, leading to overinvestment.

By shifting from duopoly to the case of N firms, Fedele et al [63] found that $I_M^*(N)$ is monotonically decreasing with N, as in the case of technical spillovers. The reason behind is that each firm gets the whole market revenue X only if all competitors are victims of security breaches, but the probability that this event occurs decreases in N. As consequence the investment in cybersecurity made in case of market spillovers is decreasingly effective with rising N. The result is that market spillovers negatively affect the per-firm equilibrium investment level.

Garcia and Horowitz [67] studied the cybersecurity corporate investment as dichotomous variable in case of market spillovers. First they considered N=2 firms which investments are I_i=[0, I] and the objective function of each one is $R_M(I_i, I_j) - I_i$. They found that moving from monopoly to duopoly, the investment is less effective (equivalent to what has been found by Kunreuther and Heal and reported above).

$$R_M(I, I) - R_M(0, I) < R_M(I,0) - R_M(0, 0)$$

The equation reported here states that the benefit in case of duopoly (left side of the equation) is lower than the benefit in case of monopoly (right side of the equation), in fact a firm has less incentive to invest in cybersecurity moving from monopoly to duopoly.

Considering now the case of N firms, Garcia and Horowitz [67] found that when N rises, the conditions under which all firms invest at the optimal level are more restrictive, since private benefit of firm i from investing in cybersecurity is represented by the difference between the revenue of the firm i in case both firm i and j invest, and the revenue of the firm i in case only firm j invests:

$$R_M(I, I) - R_M(0, I)$$

By reducing the private benefit of firm i with the loss suffered by firm j because of the reduced chance to gain the revenue share of firm i (considering that the investment of firm i reduce the probability to be attacked and consequently to lose revenue share that would go to the other firm), it is possible to find that the social benefit (i.e. the increase in the sum of the firms' payoffs when firm i decides to invest, given that firm j already invests as well) that is lower and amounts to:

$$[R_M(I, I) - R_M(0, I)] - [R_M(I,0) - R_M(I, I)]$$

As conclusion, the authors states that when the investment cost I is lower than the private benefit, firms invest at equilibrium. Since all firms under this condition would invest, this leads to overinvestment in cybersecurity with respect to the social benefit [67].

A particular focus can be done on *platforms'* market share and how the impact of security investments is influenced by strategic cyber-attacks. Literature posits that strategic attackers may find more profitable to try entering in those platforms' systems that have a larger market share. In more concentrated markets, in which platforms create a large amount of interconnections among a lot of agents in the system, an attack may be considered more profitable for attackers that target a greater amount of users and data, and this may cause dangerous damages [19].

Platforms' market share is strictly linked with the amount of investments in security: more savvy consumers buy from a platform, as more it grants security. But, at the same time, these platforms attract most attackers because of their market share. This means that larger platforms requires increasingly high investments [71].

Another interesting perspective is the one related to *complementary products* (so far it has been inspected the case of substitute products): in this case, when a firm suffers a security breach, also the firms offering the complementary product are subject to a demand reduction. This type of consequences creates the incentive for higher investments, due to the positive impact of a security investment by one firm on the revenue of the second one.

- **Demand side**

  Nagurney and Nagurney [72] observed that in case consumers are careful about cybersecurity but, due to information asymmetry, they don't know the individual firm level, they observe the average cybersecurity level of the market. In this case firms have less incentive to invest as *N* rises, since consumers are not able to distinguish firms that invest from those that do not. But, in case of a cyber-attack, the consumers start to know which are the less protected firms, that at this point lose market shares that are acquired by the competitors.

  It is possible to consider two types of customers: *switching customers* that are more sensitive to cybersecurity and in case of evidence of a scarce level of protection switch to the competitor; and *loyal customers* that are less sensitive to cybersecurity and never switch to the competitor firms.
  Qian et al [73] showed that a greater share of loyal consumer reduces competition among firms to attract switching consumers and also reduces the incentive to invest.
  Also Arce [74] considers switching consumers, with positive switching costs, finding that the higher the switching cost is, the lower is the incentive of the firm to invest in security in order to retain its market share.

- **Both technical and market spillovers**
  In this case interdependence among firms is of both technical spillovers and market spillovers. This means that are considered the firms that operate on a common computer network and that are competitors in the product market. The equilibrium

investment level decreases when N rises for any e. This result is due to two already seen effects:

- The *technical spillover effect* leads to the free-riding behaviours of firms that have no incentive to invest; as consequence the equilibrium investment is reduced when a new firm enters the network;
- The *market spillover effect* has a negative impact, because when a new firm enters the network, the probability that a firm gets the entire market revenue X decreases, leading to a reduction in the equilibrium investment level.

When both effects coexist, these two negative effects sum up and lead to the situation reported in Figure 6.

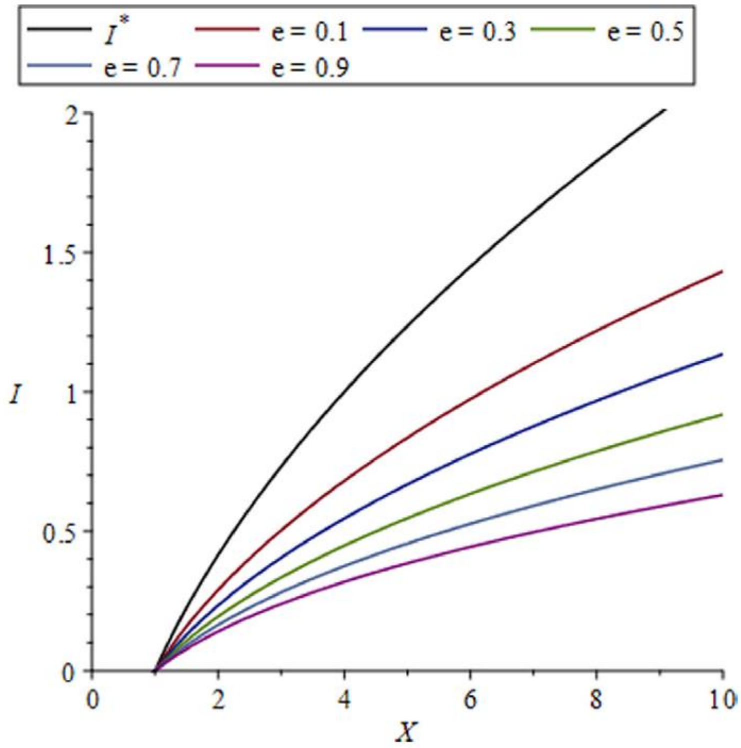

Figure 6 – Equilibrium investment with technical and market spillovers (Source: Fedele et al, *Dangerous games: A literature review on cybersecurity investments,* Journal of Economic Survey, 2022, 20)

The figure reports the different levels of equilibrium investment $I^*_{TM}(2)$ for different values of e (coloured curves), and the optimal investment level I^*(equilibrium investment level in a one-firm setting) with a=1 (black curve) as function of X. All the coloured curves are lower than I^* for any given X>1, meaning that the equilibrium investment in this case shrinks when N rises. As done for the other cases, it is possible to compare the equilibrium investment with the socially efficient level in order to understand under which conditions overinvestment or underinvestment occur. Fedele et al [63] found that lower values of e (lower incidence of technical spillovers) leads to overinvestment ($I_{TM}^{*}(2) > I_{TM}^{E}(2)$), while underinvestment ($I_{TM}^{*}(2) < I_{TM}^{E}(2)$) occurs when e rises (more prevalence of technical spillovers). This is due to the fact that market spillovers effect prevails when e is low, since the social benefit of the investment in security is lower than the private benefit due to the negative externality of market spillovers, and this leads to overinvestment. When e increases, technical spillovers produce their positive externalities and eventually prevails on market spillovers negative ones. As consequence, social benefit increases until being lower than private one, and underinvestment arises.

5. Public policy

The extent to which the cyberspace is becoming part of our reality, habits, economics, markets, social interactions, is making arise the necessity to provide a level of security and protection in this space as high as much it is in the real world, and even more. The potential damages that could arise from malicious activities online are so impactful in people's lives and could cause damages so extensive, that cybersecurity is now seen one of the responsibilities that governments take for national security. An issue in this situation is the different pace of cyber threats and cybersecurity, in fact the cyberspace is evolving rapidly and it should need to be addressed timely, but cybersecurity is one among the many problems in the agenda of the public institutions, and the progress in public policy has not be as rapid as it might have been expected [75].

In addition, the measures taken to potentially improve cybersecurity could have negative effects in other areas such as the following ones:

- Economics, due to the limited governmental budget that have to be split among all the competing demands of other bullet points in the nations' agenda;
- International relations and national security, since the non-physical national boarders of cyberspace need to face with the states and governments' measures taken by each one in terms of cybersecurity;
- Innovation, because the beneficial effects of information sharing for development of new technologies could be slowed down by privacy policies and measures for enhancement of security [40], [75].

Regarding the latter, a debate has arisen in the literature with regards to best protect privacy without harming the beneficial effect of information sharing, by considering the differences between regulation and self-regulation [40].

On one side of the debate there is the idea that companies have lost a great amount of money from online sales due to the privacy concerns of consumers, and, at the same time, consumers have had high costs due to the losses associated with identity theft, investment for protecting data, price discrimination techniques for charge higher prices on them, spam and so on. Supported by the reasons explained, the solution proposed by this side is the *regulation* addressing privacy and security issues. This solution could have the advantage to avoid the complexity encountered in case of lack of standardization among different entities, each with its own privacy policies. Privacy regulation could have both positive and negative effects, based on the attributes of laws.

On the other side, there is the idea that the costs which may arise in case of privacy violations are not as high as the costs to protect privacy, in fact it can be reported the example of targeted advertising that give useful information to customers and at the same time lead to revenues for companies in order to develop new Internet services; as consequence, it would be a cost for customers to reduce the use of online information. The solution proposed in this case is the *self-regulation*. It could be effective in case in which online operators act in a safety manner: the usage of intensive targeting of ads should be reduced if consumers' response is adverse and each online operator would follow their published policies rather than engage in spam, and in forms of price discrimination that antagonize consumers. Self-regulation mechanisms can be represented into websites by the people disclosure of their willingness not to be tracked, but limitations exist. In fact, these services often allow consumers to opt-out of advertising network, and so to not be targeted with ads, but their data are still collected by websites. The solutions proposed in self-regulation regime are related to the concepts of transparency and control and are therefore based on the individuals' ability to be informed about the use of their data, with the possibility to manage privacy settings. The base concepts often fail in the actual application due to the difficulties encountered by the privacy policies to properly inform consumers about the use of data and because those policies can nudge people to disclose information by manipulating the format in which they are written and often presented in a way in which consumers are not incentivized to read them. In addition, as presented in the previous discussion about the privacy paradox and the consumers' behaviours online, if people have control over their information, they paradoxically have more willingness to disclose them and take more risk on their privacy. In this sense, the protection can be an illusory concept. As consequence, the self-regulation solution is subject to several doubts.

Alternative approaches to privacy protection could be the *propertization* of personal information, in which there is the establishment of markets in which people can trade their data that is consider a property, or the application of *paternalistic solutions* that are designed by organization and governments to push people towards practices they have claimed to prefer.

Regulation and self-regulation can be respectively represented by the EU and US approaches, since the former provides obligations and standardization that are subject to a higher level of enforcement than the latter, which proposes more suggestions with a lower level of enforcement [40].

In this chapter there will be a focus on how the public policies influences the market competition and the social welfare frameworks, and on the institutional measures applied in the United States and European Union, with an analysis on the differences between the two approaches.

5.1.Public institutions' measures

The analysis performed before about the level of investment implemented by organizations suggests that the investment in security is not aligned with the socially optimal level and there is therefore space for interventions by governments in order to correct the distortions. De Cronière and Taylor [55] suggest three main approaches that public institutions can adopt:

- **Security standards for investment level**: the optimal level of investment analysed in the previous chapter represents the basis of the institutions suggestion that they request to respect in order to avoid under- or over- investment.
- **Financial penalties or liability for breaches**: in this case a fine is imposed by the regulators to firms that suffer a breach. This leads to an increase in the damage suffered by organisations and increases the incentive to invest more in cybersecurity countermeasures. In addition, a compensation for customers for the suffered loss can be predefined. The authors have found that in case of pricing regime, the fine and the compensation are substitutes, in fact if the compensation to customers decreases, the fine to impose to the firm needs to be higher in order to lead firms to the equilibrium investment. Instead, in advertising regime, the authors have found that the relationship between the fine and the compensation is of strategic complementarity. In this case, in fact, if the compensation for customers increases, firms have less incentive to invest in cybersecurity, and, as consequence, the regulator needs to increase the fine in order to offset this automatic mechanism and try to lead firms on the higher efficient level of investment. The difficulties encountered in this type of public policy are related to the definition of the fine and compensation amounts that would lead to the optimal level of investments. This type of measures is applied by Articles 82 and 83 of the GDPR in the European Union. It will be more detailed analysed throughout this chapter.

- **Transparency initiatives**: notification of requirements or certification schemes that can be used in order to evaluate the security level of firms and make results public. This leads to an increase of the awareness of customers about security concerns, and the share of savvy customers in the market increases. The relative consequences seen in the previous chapter in case of increase of μ are the ones that can be considered also in this case.

  In the pricing regime, the *negative network effect* (for which, as explained in the previous chapter, if more consumers choose firm *i*, the probability that it becomes a target increases, and the sophisticated consumers will consider less attractive firm *i)* is amplified by the larger share of customers with privacy concerns. In addition, due to the *competition-intensifying strategic effect* (for which, as explained in the previous chapter, if firm *i* invests in cybersecurity, it has incentives to reduce prices for the effects on both the cost and demand channels, and so, to increase the competition) the firms have less incentive to invest in security, because higher investment would lead to higher competition and reduction of prices. As consequence, in the pricing regime, a certification scheme leads to a reduction in the security level. It is useful to notice that in this case the certification scheme could have a drawback due to the more transparency. For this reason, the transparency initiatives could be coupled with a liability regime in which a larger fine is imposed to firms in case of a breach.

  In the advertising regime, instead, a certification scheme increases the equilibrium security level. This is because in this case a price has not to be set and a consequent greater attention of consumers to security (higher μ) leads firms to invest more. In this case there is a strong necessity to invest in security to attract more customers, since the certifications make security more transparent, enabling people to compare different security levels of different firms. It is necessary to notice that also in this case it is not obvious that the certification scheme is an optimal solution, because if μ is large enough firms could over invest with respect to the socially optimal level. A certification scheme in this case can be a substitute to the fine because both lead to the increase of investments.

Moving to the second framework analysed in the previous chapter, the analysis of the conditions under which underinvestment and overinvestment arise in case of technical spillovers, market spillovers and both simultaneously, there is now a focus on the tools suggested by Fedele et al. [63] that public policymakers can adopt in order to promote adequate levels of investments.

The authors reported the following three possible public tools:

- **Subsidy**: in cases in which competitors share the same computer networks but are not competitors, the technical spillovers prevail, and this is the case in which underinvestment is more likely to occur, as analysed before. Fedele et al. found that a subsidy that is function of N and e (where parameter $e \in [0,1]$ represents the positive spillovers produced by the firm i ($\neq j$) investment on security of the network, enjoyed also by firm j based on the level of interdependence among the two firms, and where N represents the number of firms in the market) would be necessary for each unit of investment I. It would lead firms toward the socially efficient level $I_T^E(N)$. The difficulties encountered in this case is that the regulator should know the market structure (N) and the level of interdependence (e).

  Instead, in case of prevalence of market spillovers, in which firms are competitors that don't share the same computer network, overinvestment arises. This could be mitigated by introducing a tax per each unit of investment I. Also in this case, there are difficulties to manage: the regulator should perfectly know the impact of the investment of each firm on the probability of a security breach, in order to make possible the internalization by firms of the negative effects arisen due to market spillovers.
- **Incentives to share information**: the difficulties of firms to estimate the precise loss due to a cyber-attack and the impact of the investment on the ex post security breach probability, yields them to select a level of investment that could be inadequate; in this case the information sharing about threats and vulnerabilities can lead to higher effectiveness of investments, in fact, if every single unit of investment is more effective, the total investment could be lower. The obstacle could be that some firms don't have interest in doing it. In order to mitigate the latter phenomenon, an incentive from the policymakers could lead firms towards these expected results.
- **Security standards regulations**: the regulators can provide quality standard for practices regarding the internal activities of firms, or the products provided to customers, even if also in this case there is still difficulty in estimating what are the good practices and standards that actually lead to adequate security levels.

Regarding the latter point, a global standard does not exist in this moment and each state adopts different approaches, some move toward a more self-regulated way to manage cybersecurity issues by providing suggestions or disclosure obligations and the requirement for minimum security standards, while others are more active in policymaking by introducing certification scheme and liability regimes for firms suffering breaches. The former case is well represented by the United States laws that has taken a more limited and sectorial regulatory approach, by providing suggestions and guidelines rather than applying enforcing principles. The latter case can be instead represented by the measures adopted by the European Union, opting for regulatory solutions by adopting enforcing principles that are related to the data collection and its use [40]. The relative regulations will be analysed in the following section, with a focus on the Italian situation too.

5.2. United States approach to cybersecurity

In the United States, there are several cybersecurity-related laws and regulations that have been introduced at the federal and state levels to address cybersecurity issues. Some of the major U.S. cybersecurity-related legislative acts are listed below:

- **Federal Information Security Modernization Act** (FISMA): this 2014 law establishes information security and cybersecurity requirements for U.S. federal agencies. FISMA requires government agencies to take steps to identify and manage cyber risks and establishes a framework for assessing and monitoring cybersecurity. It implemented new measures for the defence against cyber threats, in particular it gives the Department of Homeland Security (DHS) the authority to manage the implementation of information security policies for non-national security federal Executive Branch systems, by also providing them assistance and the necessary technologies, and it also clarifies the authority of the Office of Management and Budget (OMB) in oversighting on federal agency security practices and it assists OMB to develop those policies [76].
- **Cybersecurity and Infrastructure Security Agency Act** (CISA Act): it is a law of United States that entered in force in November 2018. CISA Act had the objective to strengthen and coordinate cybersecurity effort of the U.S. federal government. It established the federal agency called the Cybersecurity and Infrastructure Security Agency (CISA) to improve and protect the security of critical infrastructure in the

United States and to coordinate cyber emergencies response. CISA works with the private sector and government agencies to mitigate cyber threats and promote information sharing. CISA is an independent body in the Department of Homeland Security (DHS) and has the responsibilities to facilitate the information sharing in order to improve the understanding of cyber threats and to consequently develop a coordinated response; it also helps in the protection of the critical infrastructure such as energy, transport, information and communication technologies, financial sector and others, by the identification and mitigation of threats; CISA provides consulting and training services on cybersecurity practices in order to develop awareness and competencies in this field.

- **U.S. state data privacy laws:** in addition to the laws at the federal level, in the United States it is possible to identify different laws related to privacy protection based on the different states where they have been developed and they are in force. They are in particular [77]:
  - **California Privacy Right Act (CPRA):** it went into effect on January 1, 2023 and it amended and strengthened the previous California Consumer Privacy Act (CCPA).

    The CCPA was the first law in the U.S. came into effect in 2020 and it creates the basis for the following laws in the U.S. states, even if they take elements both from CCPA and European GDPR. A more detailed analysis of the CCPA characteristics and the differences with respect to the GDR will be presented below in this chapter.

    The CPRA provides additional protection on data processing and sharing. In this way, Californian people have the right to know which entities collect their data and if business sell them and to whom.
  - **Colorado Privacy Act (CPA):** this is a new law that will enter in force on July 1, 2023, and it will implement the new requirement for business of disclosing to consumers their practices in data collection and sharing. Colorado residents can also decide if opt-out of the sale of their data. In addition, the CPA imposes penalties for companies that don’t follow the rules and authorizes the state attorney general to bring enforcement actions.
  - **Maryland Online Consumer Protection Act:** the Maryland act has the objective of protecting consumers from data breaches, phishing, spyware and other cybersecurity threats. Differently from other state privacy laws,

the Maryland law is more comprehensive because, for example, it asks firms to implement procedures for avoiding unauthorized access and use of customers' personal data, and to provide the possibility to opt-out from collection, use and sell of their data. This applies to all business, also the ones out of Maryland, that collect and use data of Maryland's residents.

- **Massachusetts Data Privacy Law:** also in this case, the law is applied to all businesses, also the one outside the boundaries of the state, that hold data of Massachusetts' residents. The law requires that businesses have to obtain the consent of customers in order to collect and use their data, and they have to protect the latter. In addition, the companies have to disclose about how they use data.
- **New York Privacy Act:** New York Privacy Act is one of the most comprehensive pieces of privacy and security legislation in the United States. It imposes strict rules on the way in which companies have to manage costumers' data and also gives people new rights about data, ensuring controls on personal information. Companies in New York have been significantly impacted by this law, in fact they have to disclose which type of data they collect and use, and its purpose. It has been also provided a private right of action and civil penalties in case of violations.
- **Virginia Consumer Data Protection Act:** it is a new law entered in force on January 1, 2023, that requires companies to implement procedures in order to protect confidentiality, privacy and integrity of costumers' data. Virginia residents can also access their data and ask to correct in case of inaccuracy. The law has limits of application because it is related to businesses that collect and use data of more than 100.000 Virginia consumers or derives 50% or more of revenues from sale of customers' data.

There are significant differences between laws in each state, such as the companies affected based on where they operate and limitation on their revenues. This makes the United States approach to cybersecurity and privacy not standardized and common for all states.

In addition to the U.S. body seen above (CISA that has been established with the CISA Act in 2018), another important body in the United States in information security field is the National Institute of Standards and Technology (NIST). It is a federal agency operating under the U.S. Department of Commerce and it is responsible for the development and implementation of standards and guidelines for a wide range of areas, including technology, security and cybersecurity. NIST's primary role is to promote innovation and technological progress in the United States through the development and promotion of technical standards, security measures, and recommended practices. NIST plays a crucial role in providing guidelines for cybersecurity and information protection in the United States. NIST has developed several reference documents, such as cybersecurity guidelines (Special Publications or SPs), which provide guidance on best practices for risk management, information protection, and information systems security, such has the SP 800 series of documents, which covers a wide range of topics, including risk management, security controls, encryption, password management and many other aspects of cybersecurity. In addition, NIST also developed the Framework for Improving Critical Infrastructure Cybersecurity, known as the "NIST Framework", which consists in a set of standards, guidelines, and best practices that help organizations improve their cybersecurity risk management. The publications and standards developed by NIST are widely used in both the public and private sectors as references for assessing and improving cybersecurity and information protection. Organizations often rely on NIST guidelines and reference documents to develop cybersecurity policies, procedures and practices within their operations.

5.3.European Union approach to cybersecurity

In this chapter it will be presented a focus on the main public policies adopted in the cybersecurity field by the European Union and implemented in all the member states in order to create a common and standardized framework within the European boundaries. In EU there are several laws and regulations related to cybersecurity that have been introduced to ensure the protection of data and the security of networks and information systems. Below, it is provided a list of some of them:

- **General Data Protection Regulation (GDPR)**: The GDPR (EU Regulation 2016/679) passed in April 2016 and came into force in May 2018 in order to give firms two years to prepare. It is one of the most important and comprehensive data protection laws. This regulation is labelled “general” because it applies to all organizations that process personal data of EU citizens as well as of customers of EU-based firms with offices in EU, both offline and online. It establishes clear requirements for data security and data breach notifications, and for data collection, processing and use of it. With the GDPR, the definition of personal data is not only the personally identifiable data, but it also includes data like cookies and IP addresses. Firms have to face with two types of obligations: rights-related obligations for which they have to allow people to exercise their rights in an easy way and in a timely manner; risk-related obligations that require that firms appoint a Data Protection Officer in order to manage compliance activities. They are obliged to obtain consent from data subjects in order to handle their data, and they also have to audit internal data processes. In addition, there is the obligation to encrypt personal data and minimize data collection. Among all the others, there is also the necessity for organizations to notify in a timely manner to regulator the occurrence of a data breach and the affected individuals. GDPR requires large efforts from firms in order to be compliant with the regulation introduced and it leads to higher marginal costs for firms in collecting and using data, particularly for the collection of consent [78]. As explained above, the GDPR predefined also the imposition of fines in case of violation, that amount for 20 million euros or 4% of the global turnover, taking the larger between the two. After the entrance into force of the GDPR, the first significant fine came in January 2019, when the authorities imposed a fine of 50 million euros on Google for not having respected principles of transparency, adequate information and people consent regarding the ads personalization.

- **Network and Information Security Directive (NIS Directive)**: the EU NIS directive 2016/1148 aims to ensure a common and high level of network and information security in the European Union and it has been adopted on July 6, 2016, and member states had until May 9, 2018, to transpose it into national legislation. The Directive establishes cybersecurity requirements for essential service operators (OSEs) and digital service providers (DSPs). Essential service operators include sectors such as energy, transportation, health, water and key digital infrastructure, while digital service providers include online services such as search engines, e-commerce platforms and cloud computing services. Member states must designate a national cybersecurity authority responsible for the oversight and enforcement of the NIS at the national level. National authorities must also establish mechanisms for cooperation and information exchange among themselves and with the European Commission. The NIS requires OSEs and DSPs to take appropriate measures to manage network and information security risks and to report significant security incidents to the relevant authorities. Member states are required to establish effective, proportionate, and dissuasive penalties for violations of the NIS. The NIS Directive represents a significant effort to improve cybersecurity at the European level by promoting cooperation among member states and establishing a common regulatory framework to protect critical networks and information. Its implementation helps to strengthen cyber resilience in the European Union and mitigate cyber threats that can have a significant impact on essential service operators and digital service providers. The NIS Directive has been re-examined at the end of 2020 since its implementation was difficult, leading to fragmentation across internal market, even if it led to positive effects in organizations investment in cybersecurity [79]. It has been replaced with a new law for a common higher level of cybersecurity all around EU that has been proposed with the name of NIS2 Directive (EU NIS Directive 2022/2555). It entered in force on January 16, 2023, and the EU member states will have 21 months for transpose it into their national legislations. The legal basis of the two directives is Article 114 that establishes the internal market functioning with the approximation of national rules, but NIS2 Directive introduces more stringent supervisory measures and requirements, including security for supply chains, reporting obligations and address also the system of sanctions across EU. There are three objectives of the NIS2 Directive: increase the cyber-resilience in the European states with adequate cybersecurity measures applied by organizations, no longer divided into OESs and DSPs, but split in online marketplaces, search engines and cloud service providers; reduce inconsistencies in resilience, by aligning the de facto scope, the incident reporting requirements (by also defining a list of administrative fines in case of violation regarding reporting rules) and security requirement, the national supervision and enforcement, and the authority of the national cybersecurity organizations [80]; improve the level of collective awareness and capability to be prepared and respond to cyber-attacks, by sharing information, setting rules and procedures, and increasing the trust level with the competent authorities.

- **Cybersecurity Act** (EU Regulation 2019/881) entered into force on June 27, 2019. The EU Cybersecurity Act is a law that aims to strengthen the security of networks and information systems in the European Union. The main objective of the regulation is to harmonize cybersecurity policies in EU and promote a coordinated approach to address cyber threats. It also provides a common regulatory framework for cybersecurity certification, strengthens the role of ENISA, and promotes cooperation among member states. The regulation particularly introduced the following key elements:

- **Cybersecurity certification**: the Cybersecurity Act established a framework for the establishment of a European cybersecurity certification scheme. This allows organizations to obtain an official certification attesting to compliance with security requirements established at the EU level. The Cybersecurity Act included the creation of the "EU security certificates" which attested that IT products, services and processes meet certain security standards and can be used as evidence of compliance with security measures.
- **EU Cybersecurity Agency (ENISA):** the regulation strengthens the role of the EU Cybersecurity Agency (ENISA), providing it with increased resources and expertise to play a central role in promoting cybersecurity best practices, cooperation among member states, and technical support.
- **Cooperation among member states**: The regulation promotes greater cooperation among EU member states in the field of cybersecurity, including sharing of information on threats and vulnerabilities and collaboration in cyber crisis management.

On April 18, 2023, it has been proposed an amendment for the Cybersecurity Act for the promotion of the European certification scheme adoption for managed security services that cover the incident responses, consultancy, security audits, and penetration testing. In this way there could be a higher level of quality and reliability of the services listed which represent a critical and sensitive aspect for assisting organizations in preventing, detecting, responding and recovering to breaches [81].

- **Cyber Resilience Act:** the Cyber Resilience Act is a regulation proposal dated September 15, 2022 on cybersecurity requirements for products with digital elements in order to ensure more security in hardware and software products. It has been the consequence of studies that state these products are increasingly subject to cyber-attacks that are successful. This leads to a very high cost of cybercrime [82]. Indeed, there is a low level of cybersecurity, and users have limited information about the cybersecurity properties of the products, that could prevent them from choosing the less secure ones. The objectives of the Cyber Resilience Act are to ensure a higher level of security of products with digital elements in the whole life cycle, a common cybersecurity framework, enhancing transparency of security properties and enabling firms and people to use these products in a secure way. All EU firms should use a unique panel of security norms in order to reach the expected results. It is also expected a reduction in the number of incidents and relative administrative and reputational costs, and a higher trust between consumers and firms, potentially leading to a greater demand of these products. In addition, users will have more information about the cybersecurity profile of hardware and software, leading to a greater awareness in the product choice. The proposal also states that each member state has to appoint an authority for market monitoring that can also impose fines in case of rules violation.

The regulations are supported by specific institutions that operate in order to guarantee the applications of them. The major EU institutions are:

- **European Union Agency for Cybersecurity** (**ENISA**), an EU institution established in 2004 with the purpose of achieving a high level of cybersecurity common to all European countries. It works with organizations and business to keep EU citizens protect in the cyber space, boost the resilience of EU's infrastructures and trust in the digital products and services. In doing so, it collaborates with EU member states and institutions in order to help prepare for future cyber challenges, and it also share information, develop staff and structures and raise awareness. It was also deeply involved with the Cybersecurity Act and its application.
- **European Data Protection Board** (**EDPB**), an independent body established in 2018 in order to ensure the application in all countries of laws in this field, especially the General Data Protection Regulation (GDPR) seen above, and the Data Protection Law Enforcement Directive, (EU Directive 2016/680) entered in force on May 5, 2016 that protects natural persons' fundamental right to data protection regarding processing and free movement of personal data in case they are used by criminal law enforcement authorities. EDPB also promotes the cooperation among the national data protection authorities and advises the European Commission in case of issues related to data protection.
- **European Data Protection Supervisor** (**EDPS**), an EU body established in 2004, which ensures that EU institutions process citizens' personal information (in written, electronic or visual form) for accomplishing their duties, always in compliance with the strict privacy rules. In order to grant the safety processing of information, the EDPS supervises the EU institutions and bodies activities, works with national

authorities and monitors the emergence of new technologies that may impact data protection.

5.3.1. Italian public measures

Focusing now on the Italian situation, it is possible to notice that the cybersecurity laws apply the EU regulations. In particular:

- **Code on the Protection of Personal Data (Privacy Code):** The Privacy Code, regulated by Legislative Decree No. 196/2003 (and subsequently amended by Legislative Decree No. 101/2018), establishes the rules for the protection of personal data in Italy. It is based on the principles of the General Data Protection Regulation (GDPR) of the European Union and is in line with European legislation on personal data protection.
- **Legislative Decree No. 65/2018 (Implementation of the NIS Directive)**: it implements the European Union's Network and Information Security (NIS) Directive in Italy. It establishes obligations for essential service operators and digital service providers regarding the security of networks and information systems.

As required by the EU regulations for all the member states, Italy predefined the cybersecurity entity, the Agency for National Cybersecurity (ACN). The ACN is the National Cybersecurity Authority established by Decree Law No. 82 of June 14, 2021, to protect national interests in cyberspace. It ensures the implementation of the national cybersecurity strategy, promotes a consistent regulatory framework in the field, and exercises inspection and sanction functions; it also develops collaborations at the international level with counterpart agencies and ensures coordination among public actors and the implementation of public-private actions to ensure cybersecurity and cyber resilience.

The European Union institutions, and, as consequence, the member states institutions and organizations are working constantly for ensuring a high level of security and, as result, the public policy field is evolving over time.

5.4. Comparison between US and EU approaches

The United States and the European Union has different approaches to the cybersecurity and privacy regulations: United States has often opted for the provision of suggestions and guidelines rather that strong enforcing principles, also because, the several state laws create different approaches not often easy to harmonize and standardize. European Union has focused instead on regulatory solutions, establishing rules and principles that govern the use of data and define enforcement against the companies in case of violations.

The GDPR is one of the most impacting and comprehensive laws in Europe and represents the basis for all the national laws in terms of data protection since it provides a framework to follow for data processing. The U.S. state laws, instead, are more fragmented and more targeted in their scope. Indeed, one of the most significant differences between European and United States laws in the field in object is that in the U.S. there is not a single federal privacy law that harmonize all the state laws like the GDPR in Europe, but instead there are varying types of data protection at federal and state levels based on the different laws. In addition, in the U.S. there is an important distinction between the CCPA and the other state laws, because the CCPA was the first law in the U.S. came into effect in 2020, different from the GDPR that came into effect in EU in 2018, while the other ones have taken elements from both the GDPR and the CCPA. Also in the terms used it is possible to notice that in the CCPA there are terms such as “business”, “service provider” and “personal information”, while in the other state laws it is possible to find similarities with GDPR terms such as “controller”, “processor” and “personal data” [83].

Extending the perspective on the different U.S. state laws, including CCPA, it is possible to catch other differences with respect to the GDPR:

- **Application**: GDPR applies to any organization that process EU citizens’ personal data, regardless the location and without any limitation in terms of business revenue or processing threshold requirements. By contrast, CCPA and U.S. state laws generally apply to the businesses established in the state and that operate inside it, and they usually consider thresholds on revenues and amount of processed data (for the CCPA, for example, the entities covered are the ones with annual revenue above 25 million $, that process 50.000 or more individuals’ data and that derive 50% or more of their revenue from selling data). The U.S. states also apply other types of limitations, by exempting non-profit organizations (except for Colorado), HR and B2B data (except for California) or health information. For the reasons explained, GDPR is the most far-reaching data protection structure now, having a greater and broader application on data protection than other laws.
- **Enforcement**: GDPR imposes heavy fines against violations that amount the bigger between 20.000 million € and the 4% of global annual turnover. Data subjects can also claim a compensation in case they have been victims of a breach that caused

them material or non-material harm. In doing so, the EU is supported by the EU authorities. Among the U.S. state laws, fines range from 2.500 $ to 20.000 $ for violations. CCPA gives California residents enforcement power against companies that violate rules but limited to some type of data breaches.

- **Obligations**: differences in this area are related to the fact that GDPR also requires companies to appoint a data protection officer to oversee compliance and to establish a lawful basis for processing activities, while CCPA does not imposes these requirements. At the same time, there are similarities between the two sides: both require general obligations for businesses, related to principles of data minimisation and purpose limitation, and also define the obligation for companies to conduct a risk assessment for processing data.
- **Information**: focusing on personal information, U.S. state laws exclude publicly available information that are part of the core business for companies such as recruiters and marketers. In addition, U.S. state laws define as "de-identified" data the ones for which companies have only implemented technical and organisational measures and, for this reason, are outside scope, while GDPR requires high level standard of "anonymisation". Moving toward the sensitive information, GDPR and U.S. state laws consider the same categories as "sensitive", such as health information, genetic, biometric data, race, and religious belief. The CCPA also include information such as precise geolocation, certain types of account information, communication content etc. Related to these types of data, states such as Utah and California adopt an opt-out model, while other states such as Virginia, and Colorado has an opt-in model as the one used by the GDPR.
- **Transparency**: with respect to the transparency requested to companies about the way in which they collect, process and share information, GDPR and U.S. state laws have similar requirements. For example, they include description of processing categories and purposes and individuals' rights, but the CCPA include additional requirements such as description of categories of information sold.

The European Union and United States approaches are similar for certain aspects seen above, even if EU is characterized by strong enforcement principles, while United States one leaves more leeway in companies' actions. Both are evolving a lot in recent years due to the growing dependencies that nowadays societies have on the cyber space and to the emerging threats analysed in Chapter 2 that represent a continuous challenge for governments. Difficulties are related to the lack of knowledge about emerging technologies not still mature enough to be addressed in the right way, but, at the same time, a timely response would be the best way in order to avoid the attackers to exploit still unknown vulnerabilities and damage infrastructures and systems, especially on large scale.

6. Conclusions

In the current reality in which people's lives are strictly linked and integrated with cyberspace where everyone daily operates, any instability or challenge directly affects people. Today cybersecurity represents a requirement for organizations in order to operate in current markets, in which the security issue has reached the general interest and consumers require a higher level of data protection.

The cyberspace is the IT environment composed by interconnected networks and IT infrastructures in which people exchange information and operate daily, also characterized by its dark side in which cyber criminals carry out malicious activities for financial gains, political reasons, and sense of revenge, using several types of attacks that evolve overtime.

The factors that have influence on the cyber risk faced by organizations, could be both external and internal to firms.

The factors external to firms are the ones which organizations cannot control. It has been analysed the geographical distribution of cybercrimes, the influence of socioeconomic conditions, the role of digital infrastructures, and the consumer's risky behaviours online. It emerged that Internet acts as a force-multiplier thanks to its ubiquity characteristic, and that the positive relationship between Internet penetration and the number of cybercrime perpetrators is intensified in areas with higher education, income and lower poverty rate. This is also amplified by the availability of digital infrastructures such as broadband connections. In addition, the behaviours carried out online by users facilitate cybercriminals and increase the cyber risk.

The factors internal to firms are instead the ones that companies can manipulate with their choices. In this case it has been analysed the influence of the system concentration, the role of perceived attractiveness, Internet presence and organizational countermeasures. It has been understood that hackers tend to target larger and more centralized hubs, that, if actually attacked, could create amplified effects due to the several interdependencies they have. Since they frequently suffer breaches, the joint probability of a successful defence of the system is reduced. Therefore, smaller firms should balance, on the one hand, the higher protection level that these larger providers can offer, but on the other hand, the frequency of attacks they are subject to. Perceived attractiveness and Internet presence play a central role in the identification process of the target firm made by perpetrators, since higher perceived value and higher online visibility increases the cyber risk. The organizational countermeasures as well are fundamental in defending the system against the attempt to compromise it.

The actual directors' engagement in cybersecurity is still scarce due to the technical nature of cybersecurity and the tendency to delegate it to IT departments, leading to absence of discussions about it in Board of Directors.

The level of protection that firms provide to customers is different based on the competition environment of the market. In case of duopoly, under a pricing regime, the investment results to be lower than in case of monopoly due to the competition-intensifying effect of investment in security that does not create incentives to invest. By contrast, under the advertising regime, the investment results to be higher than in the monopoly case due to the intent of firms to avoid losing savvy customers which can go to the rival.

Other results have been observed under different types of interdependencies: in case of technical spillover effects, in which firms that are not competitors share the same computer network, underinvestment occurs. This is because each firm increasingly free rides on the other firms' investment effort and has less incentive to invest. In case of market spillover effects, in which firms are competitors but do not use a common computer network, overinvestment occurs. The reason behind is that when a firm suffers a cyber-attack, it is supposed that consumers shift to the competitor and, hence, firms tend to invest more than the socially efficient level to avoid it.

In the cases in which market is not able to find the equilibrium on its own, public policies can act as moderators to move investment towards the optimal level. The main approaches for this purpose are the application of minimum security standards, financial penalties and consumers' compensations, transparency initiatives (such as certification scheme), and subsidy. Both European Union and United States, despite the different approaches, applied these measures in order to increase national infrastructures security and data protection online.

References

[1] C. Biancotti, «Cyber Attacks: Preliminary Evidence from the Bank of Italy's Business Surveys», *SSRN Electron. J.*, 2017, doi: 10.2139/ssrn.2954991.

[2] «SolarWinds hack explained: Everything you need to know», *WhatIs.com*. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (consultato 22 giugno 2023).

[3] European Network and Information Security Agency., *NIS investments.* LU: Publications Office, 2020. Consultato: 27 giugno 2023. [Online]. Disponibile su: https://data.europa.eu/doi/10.2824/50973

[4] Y. Li e Q. Liu, «A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments», *Energy Rep.*, vol. 7, pp. 8176–8186, nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[5] M. K. Rogers, «A two-dimensional circumplex approach to the development of a hacker taxonomy», *Digit. Investig.*, vol. 3, fasc. 2, pp. 97–102, giu. 2006, doi: 10.1016/j.diin.2006.03.001.

[6] J. V. Beveren, «A CONCEPTUAL MODEL OF HACKER DEVELOPMENT AND MOTIVATIONS», vol. 1, fasc. 2, 2001.

[7] M. Csikszentmihalyi, *Flow: The psychology of optimal experience*. New York: Harper & Row., 1990.

[8] A. Bandura, *Social learning theory.* Englewood Cliffs, NJ: Prentice Hall., 1977.

[9] M. K. Rogers, «The Psyche of Cybercriminals: A Psycho-Social Perspective», in *Cybercrimes: A Multidisciplinary Analysis*, S. Ghosh e E. Turrini, A c. di, Berlin, Heidelberg: Springer, 2011, pp. 217–235. doi: 10.1007/978-3-642-13547-7_14.

[10] S. Chng, H. Y. Lu, A. Kumar, e D. Yau, «Hacker types, motivations and strategies: A comprehensive framework», *Comput. Hum. Behav. Rep.*, vol. 5, p. 100167, mar. 2022, doi: 10.1016/j.chbr.2022.100167.

[11] «What is Cyber Attack Meaning? Types and Examples». https://www.wallarm.com/what/what-is-a-cyber-attack (consultato 17 aprile 2023).

[12] «What is a DDoS botnet?», *Cloudflare*. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/ (consultato 17 aprile 2023).

[13] «Google says it stopped the largest DDoS attack ever recorded in June». https://therecord.media/google-says-it-stopped-the-largest-ddos-attack-ever-recorded-in-june (consultato 17 aprile 2023).

[14] A. Dizdar, «SQL Injection Attack: Real Life Attacks and Code Examples», *Bright Security*, 8 aprile 2022. https://brightsec.com/blog/sql-injection-attack/ (consultato 17 aprile 2023).

[15] «What is a Zero-Day Exploit | Protecting Against 0day Vulnerabilities | Imperva», *Learning Center*. https://www.imperva.com/learn/application-security/zero-day-exploit/ (consultato 17 aprile 2023).

[16] «What is Phishing Attack? Types and Examples». https://www.wallarm.com/what/types-of-phishing-attacks-and-business-impact (consultato 17 aprile 2023).

[17] «What is Malware? Types and Examples». https://www.wallarm.com/what/malware-types-and-detection (consultato 17 aprile 2023).

[18] «What is Malware | Malware Detection and Removal | Imperva», *Learning Center*. https://www.imperva.com/learn/application-security/malware-detection-and-removal/ (consultato 17 aprile 2023).

[19] D. Geer, E. Jardine, e E. Leverett, «On market concentration and cybersecurity risk», *J. Cyber Policy*, vol. 5, fasc. 1, pp. 9–29, gen. 2020, doi: 10.1080/23738871.2020.1728355.

[20] European Union Agency for Cybersecurity., *Identifying emerging cybersecurity threats and challenges for 2030.* LU: Publications Office, 2023. Consultato: 17 giugno 2023. [Online]. Disponibile su: https://data.europa.eu/doi/10.2824/117542

[21] J. Park, D. Cho, J. K. Lee, e B. Lee, «The Economics of Cybercrime: The Role of Broadband and Socioeconomic Status», *ACM Trans. Manag. Inf. Syst.*, vol. 10, fasc. 4, pp. 1–23, dic. 2019, doi: 10.1145/3351159.

[22] Y. Bakos e E. Brynjolfsson, «Bundling Information Goods: Pricing, Profits, and Efficiency», *Manag. Sci.*, vol. 45, fasc. 12, pp. 1613–1630, dic. 1999, doi: 10.1287/mnsc.45.12.1613.

[23] M. Kelly, «Inequality and Crime», 2000.

[24] V. Benjamin, B. Zhang, J. F. Nunamaker, e H. Chen, «Examining Hacker Participation Length in Cybercriminal Internet-Relay-Chat Communities», *J. Manag. Inf. Syst.*, vol. 33, fasc. 2, pp. 482–510, apr. 2016, doi: 10.1080/07421222.2016.1205918.

[25] N. Kshetri, «The simple economics of cybercrimes», *IEEE Secur. Priv.*, vol. 4, fasc. 1, pp. 33–39, gen. 2006, doi: 10.1109/MSP.2006.27.

[26] S. Raphael e R. Winter-Ebmer, «Identifying the Effect of Unemployment on Crime», ago. 1998, Consultato: 17 aprile 2023. [Online]. Disponibile su: https://escholarship.org/uc/item/5hb4h56g

[27] L. Abrardi e C. Cambini, «Ultra-fast broadband investment and adoption: A survey», *Telecommun. Policy*, vol. 43, fasc. 3, pp. 183–198, apr. 2019, doi: 10.1016/j.telpol.2019.02.005.

[28] J. Turow, J. King, C. J. Hoofnagle, A. Bleakley, e M. Hennessy, «Americans Reject Tailored Advertising and Three Activities that Enable It». Rochester, NY, 29 settembre 2009. doi: 10.2139/ssrn.1478214.

[29] M. Madden e L. Rainie, «Americans' Attitudes About Privacy, Security and Surveillance», mag. 2015, Consultato: 30 aprile 2023. [Online]. Disponibile su: https://policycommons.net/artifacts/619110/americans-attitudes-about-privacy-security-and-surveillance/1600177/

[30] J. P. Carrascal, C. Riederer, V. Erramilli, M. Cherubini, e R. de Oliveira, «Your browsing behavior for a big mac: economics of personal information online», in *Proceedings of the 22nd international conference on World Wide Web*, in WWW '13. New York, NY, USA: Association for Computing Machinery, mag. 2013, pp. 189–200. doi: 10.1145/2488388.2488406.

[31] B. Brown, «Studying the internet experience», 2001.

[32] A. Acquisti e J. Grossklags, «Privacy and rationality in individual decision making», *IEEE Secur. Priv.*, vol. 3, fasc. 1, pp. 26–33, gen. 2005, doi: 10.1109/MSP.2005.22.

[33] S. B. Barnes, «A privacy paradox: Social networking in the United States», *First Monday*, set. 2006, doi: 10.5210/fm.v11i9.1394.

[34] M. Grobler e J. J. van Vuuren, «Broadband broadens scope for cyber crime in Africa», in *2010 Information Security for South Africa*, Johannesburg, South Africa: IEEE, ago. 2010, pp. 1–8. doi: 10.1109/ISSA.2010.5588287.

[35] A. Acquisti, «Privacy in electronic commerce and the economics of immediate gratification», in *Proceedings of the 5th ACM conference on Electronic commerce*, in EC '04. New York, NY, USA: Association for Computing Machinery, mag. 2004, pp. 21–29. doi: 10.1145/988772.988777.

[36] S. Kokolakis, «Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon», *Comput. Secur.*, vol. 64, pp. 122–134, gen. 2017, doi: 10.1016/j.cose.2015.07.002.

[37] T. Dinev e P. Hart, «An Extended Privacy Calculus Model for E-Commerce Transactions», *Inf. Syst. Res.*, vol. 17, fasc. 1, pp. 61–80, mar. 2006, doi: 10.1287/isre.1060.0080.

[38] Z. (Jack) Jiang, C. S. Heng, e B. C. F. Choi, «Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions», *Inf. Syst. Res.*, vol. 24, fasc. 3, pp. 579–595, set. 2013, doi: 10.1287/isre.1120.0441.

[39] H. Xu, X. (Robert) Luo, J. M. Carroll, e M. B. Rosson, «The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing», *Decis. Support Syst.*, vol. 51, fasc. 1, pp. 42–52, apr. 2011, doi: 10.1016/j.dss.2010.11.017.

[40] A. Acquisti, C. Taylor, e L. Wagman, «The Economics of Privacy», *J. Econ. Lit.*, vol. 54, fasc. 2, pp. 442–492, giu. 2016, doi: 10.1257/jel.54.2.442.

[41] A. Acquisti, S. Gritzalis, e C. Lambrinoudakis, «What Can Behavioral Economics Teach Us about Privacy?», in *Digital Privacy*, Auerbach Publications, 2007.

[42] Y. M. Baek, E. Kim, e Y. Bae, «My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns», *Comput. Hum. Behav.*, vol. 31, pp. 48–56, feb. 2014, doi: 10.1016/j.chb.2013.10.010.

[43] C. Jensen, C. Potts, e C. Jensen, «Privacy practices of Internet users: Self-reports versus observed behavior», *Int. J. Hum.-Comput. Stud.*, vol. 63, fasc. 1, pp. 203–227, lug. 2005, doi: 10.1016/j.ijhcs.2005.04.019.

[44] A. Acquisti e J. Grossklags, «Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior», 2003.

[45] S. Barth e M. D. T. de Jong, «The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review», *Telemat. Inform.*, vol. 34, fasc. 7, pp. 1038–1058, nov. 2017, doi: 10.1016/j.tele.2017.04.013.

[46] R. Congiu, L. Sabatino, e G. Sapi, «The Impact of Privacy Regulation on Web Traffic: Evidence From the GDPR.», *Inf. Econ. Policy*, vol. 61, p. 101003, dic. 2022, doi: 10.1016/j.infoecopol.2022.101003.

[47] L. Anthony (Tony)Cox Jr, «What's Wrong with Risk Matrices?», *Risk Anal.*, vol. 28, fasc. 2, pp. 497–512, 2008, doi: 10.1111/j.1539-6924.2008.01030.x.

[48] A. Coburn, E. Leverett, e G. Woo, *Solving Cyber Risk: Protecting Your Company and Society*. John Wiley & Sons, 2018.

[49] «The world's most valuable resource is no longer oil, but data», *The Economist*, 2017. Consultato: 29 aprile 2023. [Online]. Disponibile su: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[50] S. Ransbotham e S. Mitra, «Choice and Chance: A Conceptual Model of Paths to Information Security Compromise», *Inf. Syst. Res.*, vol. 20, fasc. 1, pp. 121–139, mar. 2009, doi: 10.1287/isre.1080.0174.

[51] M. Swanson, J. Hash, e P. Bowen, «Guide for Developing Security Plans for Federal Information Systems», National Institute of Standards and Technology, NIST Special Publication (SP) 800-18 Rev. 1, feb. 2006. doi: 10.6028/NIST.SP.800-18r1.

[52] S. E. Schechter e M. D. Smith, «How Much Security Is Enough to Stop a Thief?», in *Financial Cryptography*, R. N. Wright, A c. di, in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2003, pp. 122–137. doi: 10.1007/978-3-540-45126-6_9.

[53] M. T. Siponen, «Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods», *Inf. Organ.*, vol. 15, fasc. 4, pp. 339–375, ott. 2005, doi: 10.1016/j.infoandorg.2004.11.001.

[54] J. Furman, D. Coyle, A. Fletcher, e P. Marsden, «Unlocking digital competition, Report of the Digital Competition Expert Panel», mar. 2019, doi: https://doi.org/10.17639/wjcs-jc14.

[55] A. de Corniere e G. Taylor, «Data and Competition: a Simple Framework, with Applications to Mergers and Market Structure», 2021.

[56] Q.-J. Yeh e A. J.-T. Chang, «Threats and countermeasures for information system security: A cross-industry study», *Inf. Manage.*, vol. 44, fasc. 5, pp. 480–491, lug. 2007, doi: 10.1016/j.im.2007.05.003.

[57] R. von Solms, H. van der Haar, S. H. von Solms, e W. J. Caelli, «A framework for information security evaluation», *Inf. Manage.*, vol. 26, fasc. 3, pp. 143–153, mar. 1994, doi: 10.1016/0378-7206(94)90038-8.

[58] A. Bendovschi, «Cyber-Attacks – Trends, Patterns and Security Countermeasures», *Procedia Econ. Finance*, vol. 28, pp. 24–31, 2015, doi: 10.1016/S2212-5671(15)01077-1.

[59] A. Tsohou, V. Diamantopoulou, S. Gritzalis, e C. Lambrinoudakis, «Cyber insurance: state of the art, trends and future directions», *Int. J. Inf. Secur.*, gen. 2023, doi: 10.1007/s10207-023-00660-8.

[60] M. Gale, I. Bongiovanni, e S. Slapnicar, «Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead», *Comput. Secur.*, vol. 121, p. 102840, ott. 2022, doi: 10.1016/j.cose.2022.102840.

[61] R. Anderson e T. Moore, «The Economics of Information Security», *Science*, vol. 314, fasc. 5799, pp. 610–613, ott. 2006, doi: 10.1126/science.1130992.

[62] A. de Cornière e G. Taylor, «A Model of Information Security and Competition», 2021.

[63] A. Fedele e C. Roner, «Dangerous games: A literature review on cybersecurity investments», *J. Econ. Surv.*, vol. 36, fasc. 1, pp. 157–187, feb. 2022, doi: 10.1111/joes.12456.

[64] L. A. Gordon e M. P. Loeb, «The economics of information security investment», *ACM Trans. Inf. Syst. Secur.*, vol. 5, fasc. 4, pp. 438–457, nov. 2002, doi: 10.1145/581271.581274.

[65] H. Kunreuther e G. Heal, «Interdependent Security», *J. Risk Uncertain.*, vol. 26, fasc. 2–3, pp. 231–49, 2003.

[66] H. Varian, «System Reliability and Free Riding», in *Economics of Information Security*, L. J. Camp e S. Lewis, A c. di, in Advances in Information Security. Boston, MA: Springer US, 2004, pp. 1–15. doi: 10.1007/1-4020-8090-5_1.

[67] A. Garcia e B. Horowitz, «The potential for underinvestment in internet security: implications for regulatory policy», *J. Regul. Econ.*, vol. 31, fasc. 1, pp. 37–55, feb. 2007, doi: 10.1007/s11149-006-9011-y.

[68] J. Willemson, «On the Gordon&Loeb Model for Information Security Investment», 2006.

[69] M. Lelarge e J. Bolot, «Network externalities and the deployment of security features and protocols in the internet | ACM SIGMETRICS Performance Evaluation Review», 2008. https://dl.acm.org/doi/abs/10.1145/1384529.1375463 (consultato 17 maggio 2023).

[70] J. Grossklags, N. Christin, e J. Chuang, «Secure or insure? a game-theoretic analysis of information security games», in *Proceedings of the 17th international conference on World Wide Web*, in WWW '08. New York, NY, USA: Association for Computing Machinery, apr. 2008, pp. 209–218. doi: 10.1145/1367497.1367526.

[71] A. J. O'Donnell, «When Malware Attacks (Anything but Windows)», *IEEE Secur. Priv.*, vol. 6, fasc. 3, pp. 68–70, mag. 2008, doi: 10.1109/MSP.2008.78.

[72] A. Nagurney e L. S. Nagurney, «A game theory model of cybersecurity investments with information asymmetry», *NETNOMICS Econ. Res. Electron. Netw.*, vol. 16, fasc. 1, pp. 127–148, ago. 2015, doi: 10.1007/s11066-015-9094-7.

[73] X. Qian, J. Pei, X. Liu, M. Zhou, e P. M. Pardalos, «Information security decisions for two firms in a market with different types of customers», *J. Comb. Optim.*, vol. 38, fasc. 4, pp. 1263–1285, nov. 2019, doi: 10.1007/s10878-019-00446-6.

[74] D. G. Arce M. e T. Sandler, «Counterterrorism: A Game-Theoretic Analysis», *J. Confl. Resolut.*, vol. 49, fasc. 2, pp. 183–200, 2005.

[75] National Research Council *et al.*, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington, D.C., UNITED STATES: National Academies Press, 2014. Consultato: 30 maggio 2023. [Online]. Disponibile su: http://ebookcentral.proquest.com/lib/polito-ebooks/detail.action?docID=3379336

[76] «Federal Information Security Modernization Act | CISA». https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act (consultato 10 giugno 2023).

[77] «U.S. Privacy Laws: The Complete Guide | Varonis». https://www.varonis.com/blog/us-privacy-laws (consultato 10 giugno 2023).

[78] S. Goldberg, G. Johnson, e S. Shriver, «Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic &amp; E-Commerce Outcomes», *SSRN Electron. J.*, 2019, doi: 10.2139/ssrn.3421731.

[79] «NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist», *ENISA*. https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist (consultato 4 giugno 2023).

[80] «The NIS2 Directive: A high common level of cybersecurity in the EU | Think Tank | European Parliament». https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333 (consultato 4 giugno 2023).

[81] «The EU Cybersecurity Act | Shaping Europe's digital future», 25 maggio 2023. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (consultato 4 giugno 2023).

[82] «Cyber Resilience Act | Shaping Europe's digital future», 15 settembre 2022. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act (consultato 4 giugno 2023).

[83] «GDPR vs U.S. state privacy laws: How do they measure up?», *Fieldfisher*. https://www.fieldfisher.com/en/insights/gdpr-vs-u-s-state-privacy-laws-how-do-they-measure (consultato 10 giugno 2023).

Acknowledgments

I would like to offer my sincere thanks to Professor Carlo Cambini for his availability from the first moment and the constant help throughout the development of the thesis.

A great thank is for my family who supported me from the beginning of this path by always inviting me to live the university with extreme serenity and in the healthiest possible way.

I am deeply grateful to Matteo, who has always supported me, most of all in the last period, sharing with me the same difficulties and worries. The fact that we end together this long path makes me very happy.

I would like to say thank you to all my friends because each one has had an important role in this path, as well as in my life.

A special thanks to my colleagues because during the time passed together since September their presence at work has always been very helpful for me.