Università Cattolica del Sacro Cuore di Milano

FACOLTÀ DI SCIENZE BANCARIE,
FINANZIARIE E ASSICURATIVE

Corso di Laurea in Statistical and Actuarial Sciences

MODELLING CYBERSECURITY INSURANCE

Relatore
Prof. Gian Paolo Clemente

Tesi di Laurea di
Saverio BELVEDERE
Matricola: 5004205

Anno Accademico 2021-2022

"All we have to decide is what to do with the time that is given us."

J.R.R. Tolkien

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The purpose of this dissertation is a pricing proposal for an annual cyber policy for small to medium-sized enterprises. As will be explained later, in Europe, and more specifically in Italy, this type of policy is still little known and widespread, but the risks covered by the policy are many and are increasing year by year. Being a relatively recently distributed and sold policy, there are still few papers in the literature that deal with pricing it. The two main approaches are pricing from a "macro" point of view, using for example the collective risk model, which is widely used for other lines of business, or from a "micro" point of view, which will be the methodology developed in the following.

The micro point of view means investigating the interactions between device/servers during the contractual term, trying to reconstruct and simulate possible infections and damages in order to obtain a premium. To do this, an epidemiological model will be introduced and used to have a criterion for infections within the company in question. The model used in the literature is known as *heterogeneous generalised susceptible-infectious-susceptible* (HG-SIS) and is a generalisation of the SIS and $\varepsilon - SIS$ model. In this way, given a time instant, a computer can either be infected or susceptible to infection. In the second case, if it is infected, the computer changes state, suffers a certain loss (amount of interest from an actuarial point of view) and needs a certain period of time to recover and restore full operation.

The peculiarity of this epidemiological model is that a device can be susceptible to either internal attacks (i.e. from other devices within the company) or external attacks (i.e. a *phishing* attack). A simulative approach was therefore used using R software, both to generate the network of devices being priced and for the epidemiological model.

The dissertation is organised as follows:

- Chapter 2 provides a comprehensive definition of Cyber Risk that underlies the needs of the cyber insurance market. The need for cyber insurance from an economic and social perspective is then justified. Subsequently, an overview of Italy is given from the point of view of the most commonly used attacks against companies and critical infrastructures and the most widespread policies. Subsequently, cyber risk is presented from the perspective of Solvency II, thus from the point of view of both non-life underwriting risk and operational risk.

  Finally, the chapter concludes by explaining silent cyber covers and then describing the limitations that already exist in the market, concerning cyber risk, without sales of *ad-hoc* policies.

- Chapter 3 consists of a proposal for a one-year contract. It then lays the mathematical and methodological foundations for pricing. Accordingly, it provides a brief introduction to graph theory and describes how to schematise the structure and interconnections within a company. It then describes a function to generate a network (e.g. using the Erdos-Renyi algorithm) with desired characteristics. All statistical distributions are then presented with their characteristics required for the implementation of the infection dynamics of the epidemiological model.

  Loss cost functions and recovery cost functions are then illustrated to capture the economic losses resulting from the infection and recovery of nodes (once infected). Finally, the simulation algorithm is presented (via pseudocode).

- Chapter 4 presents two case studies, illustrating the network topology and the results obtained through the simulation algorithm.

- Conclusions: a summary is made of the results obtained with the presented approach and possible future developments and limitations are presented.

Chapter 2

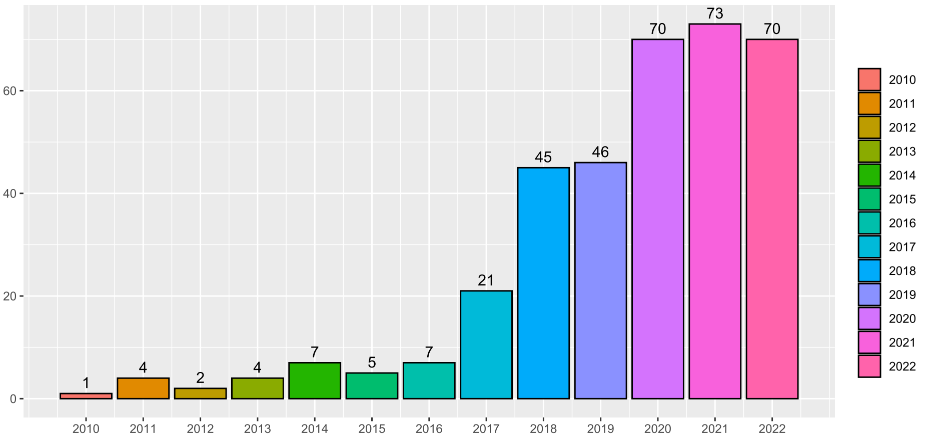
Cyber Risk & Cyber Insurance

2.1 A comprehensive definition of Cyber Risk

In this section, an attempt will be made to give a comprehensive definition of cyber risk. Over the years, numerous definitions of cyber risk have been given, as the problem and the topic in general are addressed by a multiplicity of sources and actors. The issue of cyber risk can be addressed by computer science, behavioural sciences, institutional investors, financial and insurance entities, research organisations and each of them tends to analyse one side of the argument.
As can be seen in the Figure 2.1, the number of results on Scopus[1] containing the keyword "cyber risk" has been increasing over the years and almost every one of these results has a slightly different definition of cyber risk. In [25], the author considered the literature in recent years from various sources and analysed all the definitions provided.

Examples of definitions are the one provided by [13] which defines cyber risk as "a combination of the probability of an event in the field of network information systems and the effects of this event on assets and reputation of an organisation". In [4] cyber risk is defined "as a breach of integrity and failure of information & communication technology systems (ICT)". To select and identify the right definition of cyber risk, it is necessary to incorporate numerous definitions found in the literature

[1] `https://www.scopus.com/`



Source: Scopus

Figure 2.1: Number of results on Scopus searching "cyber risk".

and identify the commonalities between them. According to [25], there are in fact *one-dimensional*, *two-dimensional* or *comprehensive* definitions. In a one-dimensional definition, only one aspect is taken into account. One can focus on the *sources* of cyber risk rather than on the *objects* of cyber risk or the *impact* of cyber risk. In two-dimensional definitions, on the other hand, the interactions of the three previous elements are considered. Comprehensive definitions can also be found in the literature, but they are very rare.

The aspects taken into consideration are thus the *sources* of cyber risk, cyber risk *objects* and the *impact* of cyber risk. The reasons are quickly stated. Correctly speaking of sources helps to generalise the possible dangers of cyber risk. Today, in fact, there is a tendency to speak of *cyber-space* and not only of "internet" as the source of cyber risk. Speaking instead of the objects of cyber risk, they can be of the most varied nature. They can be physical or non-physical. Examples of objects are telecommunications equipment, machines, servers, computers, Internet sites, cars, mobile phones etc. In the era of the *internet of things*, the potential objects targeted by cyber threats are a multitude. This is why one must be sufficiently general when speaking of cyber threats. The impact of cyber risk can be disruptive. There can be an impact on a company's functions, image or reputation. There can be an impact on the resources or privacy of the company's workers and customers. Only by thoroughly investigating all possible aspects of this risk is it possible to implement all defence mechanisms and actions.

The comprehensive definition provided by the author in [25] is the following.

Definition 2.1.1 (Cyber risk)**.** It is an *operational risk* associated with performance of activities in the cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption or reputational harm. The term 'cyber risk' also includes physical threats to the ICT resources within organisation.

The first thing that must be emphasised is that it is defined as an operational risk. This is very important because it is possible for this risk to be analysed and addressed by the companies in a quite common framework. Furthermore, it is possible to extend the studies already done over the years on operational risk to cyber risk as well. Consider, for example, the scarcity of databases on cyber risk. Subsequently, proven operational risk modelling methods for the purpose of cyber risk could also potentially be applied. Furthermore, it should also be noted that the definition provided above incorporates all three important aspects: source of cyber risk, object and impact of cyber risk.

As the concept cyber risk is multifaceted, a definition, even a comprehensive one, is not sufficient to avoid ambiguity. In the IT literature, there is a constant focus, for instance, on the use of *ontologies*. To describe them briefly, one can speak of being like a sort of "glossary" in which an attempt is made to define, with increasing specificity and precision, each term that makes up a definition. The contents of a definition then relate to each other and this set of concepts and relations provides a *meta-model*. In [25], the author has provided a meta-model for cyber risk and will be mentioned below. First, it is useful to describe the scheme of the meta-model. As can be seen from the Image 2.2 a possible threat, originates from four main parameters. These are the sources, the motives, the actor and the location. More formally, a threat can be defined as a potential cause of a cyber incident that

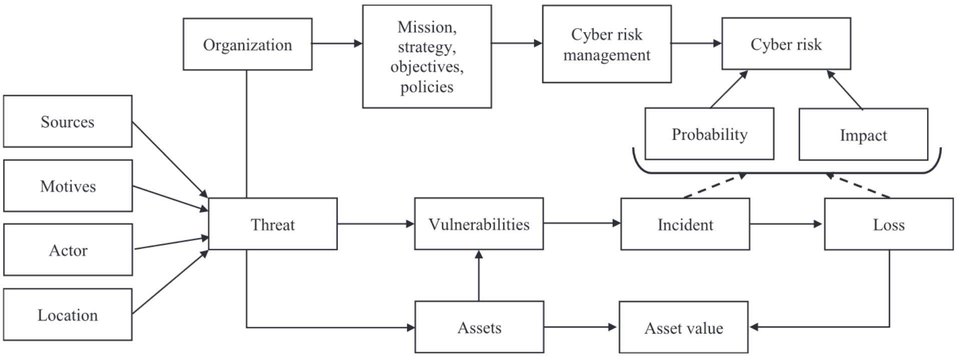


Figure 2.2: An example of an ontological metamodel for cyber risk.

could result in a loss for the company or entity in question [14]. Speaking instead of the source of the threat, it may originate from *within* or *outside* the organisation and is closely interconnected with the perpetrator/author. The main distinction for the author of the threat is whether it is a human entity or a natural event. Although they are much rarer, it may happen that a cyber incident is linked to a natural incident such as a flood or a fire of a non-intentional nature. More commonly, the perpetrator of the incident may be an employee of the organisation, a customer or a former employee. Then there can be threats from organised crime or even from states acting through hackers and agencies that specialise in cyber attacks. According to [14], this can also include computer-assisted fraud, espionage, sabotage and vandalism. The important aspect to emphasise is that, given a threat, if there is any weakness or flaw in the company's assets, it can translate into a vulnerability. Vulnerabilities, however, in the vast majority of cases, do not result in an incident and consequently a loss for the company. There are many potential vulnerabilities that are not exploited by malicious attackers. As can be seen in the scheme, the combination of the probability of an incident and its negative impact (loss) form the cyber risk.

Once there is awareness of the presence of vulnerabilities and threats, the organisation comes into play, which, thanks to a process of analysis and study, elaborates a mission, a strategy and finalises objectives and policies to manage them. Given the complexity of a company's organisational structures, the number of agents involved on a daily basis, and given the complexity and difficulty of the processes that involve the daily routine of an entity, it is impossible to solve and "zero in on" the risk. A trivial reason for this is that new threats continually arise and, consequently, new possible vulnerabilities become known every day and the time to react is not immediate. In addition, there is always a budget constraint that often prevents one from being able to allocate as many resources as one would like. It is also true that the degree of awareness of companies with regard to cyber risk is still very, very low and many things can be done to mitigate this risk, e.g. a customised cyber insurance policy.

2.2 The need for cyber insurance policies

The previous section discussed the possible actions an entity can take to mitigate cyber risk, which, as mentioned earlier, can have a disrupting impact. One of these actions is a cyber insurance policy. This section will present cyber policies in general and what their limitations and possible developments are. It will also outline possible actions needed on the part of the legislator to improve the environment within which cyber policies (and its actors) fit.

Although there are many types of cyber policies, the market is very *concentrated*. Some sources such as [17] and [22] report that as much as 90 % of all premiums for cyber policies come from the US and the remaining 10% of premiums are split between Europe and Asia. In itself, this data is already very interesting because it shows how even in developed countries and with a fairly mature insurance market, there is still an underestimation of cyber knowledge and much less policy underwriting activity. Then there are entire countries totally lacking in adequate cyber coverage which, from a global supply chain perspective, can have effects that affect upstream companies.

It is also possible to analyse where these insurance premiums come from. The most recent data from the US says that about half of all companies have some form of cyber policy and that this percentage is increasing. The percentages of the reports that can be consulted vary from report to report. Unfortunately in this type of publication there is often a large *selection bias* and consequently very different samples from each other. But what can always be appreciated is the *trend*. It is immediately noticeable that alongside the growing academic interest in the topic of cyber risk and cyber insurance (see Figure 2.1), there is also a growing interest from the perspective of the insurance business.

Usually when people talk about cyber policies they refer to large companies that have the knowledge and means to be able to buy adequate ones. Instead, the greatest impact according to many authors (e.g. [17]) would be on small and medium-sized companies (hereafter referred to as SMEs). This is because in countries (such as Italy) they are the vast majority of companies and because, despite the efforts of governments and policy makers, there has not yet been sufficient awareness of this segment of companies.

There is also a false belief that SMEs are less affected than large companies. This claim, however, has been significantly refuted by reports such as Verizon's [27]. For example, referring to data breaches alone, the report shows that out of 5212 breaches that occurred in 2022 alone, as many as 715 (13.7%) occurred in small companies. It is good to remember that it is extremely difficult to be able to trace the data breach back to the type of company. Referring then to "known" breaches, this percentage jumps to 73%. In support of this claim, the insurance broker SATEC[2] also reported that, in the Italian market alone, an estimated 43.7% of companies with fewer than 50 employees in Italy have reported *at least* one cyber attack, and the percentage is rising.

The reasons why there is little interest from SMEs are many and the following aspects do not claim to be exhaustive. First of all, in order to even take an interest in a cyber policy, there needs to be an insurance culture and product knowledge. It is therefore more likely that these types of policies are more prevalent in countries with a developed and mature insurance sector than in developing countries or where the insurance sector is immature and not ready. Once the interest in the cyber policy has been shown, the entity immediately encounters a process that is far from simple. On the one hand, there is the insurance company's need to have

[2] `https://www.satecunderwriting.eu/en/`

as much information as possible in order to catalogue/cluster the potential customer and to be able to make a good pricing. On the other hand, there is the desire of underwriters to have a streamlined process that does not discourage policyholders. It is important to keep in mind that it is normal for large companies to be required by insurers to go through an audit process aimed at clearing up any doubts about the company and to put in place whatever is necessary to avoid the claim e.g. updating systems, changing something in their organisation etc. These audits are simply too expensive for SMEs and it is common insurance practice not to request any specific data for smaller entities, otherwise the insurance premium would go up so much in price that it would discourage any smaller policyholder.

Furthermore, insurance policies are also very complex contracts, and there is no common standard on the terms to be included. They are also full of clauses and exclusions, making them difficult to compare and it is difficult for a potential policyholder to tell whether it is a good policy or not (e.g. considering deductibles). On the insurers' side, there is a desire to be able to have all the legal tools they need to protect themselves in court or in a litigation. The problem with all these exclusions is that, if the perception increases on the policyholder side that insurers will always find an excuse for not having their claim indemnified, it is likely that there will be *adverse selection* in the portfolio and only bad quality policyholders will remain within it.

Another reason why SMEs (and in general entities that are not inclined to innovate) do not show much interest in cyber policies is that there is a widespread belief that because their day-to-day activities are not very computerised, then they so there is no reason to worry too much about cyber risk. This belief is wrong. Consider, for example, a small business that handles payments or health data and has to deal with POS. These tools, like any electronic tool, have a software and hardware component and can exhibit vulnerabilities that can be exploited and cause harm if sensitive customer data is revealed. In addition, one can be a victim of phishing by also only managing vendor relationships and dealing with an email client.

Until a few years ago it was also thought that sectors such as manufacturing, for example, were less prone to cyber attacks, but data are increasingly disproving this claim. The reasons for this are many. For one thing, business processes are becoming increasingly computerised. Consider also the contribution made by Covid in recent years to migrate to a growing share of smart working workers. This shift has taken place very hastily and without often taking into account the risks involved. In addition, financial, insurance and all entities that do more "office" work were already prepared and quite ready for a massive migration to smart working. Realities such as manufacturing, on the other hand, lagged behind and found themselves unprepared from the perspective of governance, risk management and IT infrastructure. Referring to specific events, the Carraro Group, a leading Italian company in the agricultural machinery manufacturing sector, was forced to apply for layoffs (redundancy funds) for about 700 workers in 2020. The reason was quickly stated: due to a cyber attack, both production and administrative facilities had been paralysed, making it impossible for a large part of the workers to carry out normal work activities.

So how can companies be enticed toward cyber coverage and greater resilience? Approaches can come from the insurance business side or from the government and legislator side, and it is essential that these two approaches communicate and know how to create synergies. The first approach will be briefly discussed below, while the second approach will be explored more in the next section. From a business perspective, the main effort is to target possible cyber insurance products to two broad categories of policyholders: small businesses and large corporations. The insurance broker SATEC, for example, distinguishes its insurance offerings in this way. For the first group, SMEs, policies are "pre-tariffed" and it is sufficient to fill out questionnaires and provide all the necessary information. The vocabulary used is relatively simple. The second type of policies is a "quoted" product i.e. customised to the individual company. The main reason is that large companies, given their structure and the level of resources already allocated to the IT department, allow for a more detailed analysis. For example, external and internal tools are used by the broker and/or insurer that allow a comprehensive view of all possible vulnerabilities in the company. Contextually, there is a continuous dialogue between the two parties so as to improve what are the critical points.

Each policy then is activated by a *trigger* that is well defined in the contract. It is good to remember that in insurance practice it is common to distinguish large from small companies using revenues and not solely the number of employees. Thresholds are chosen, such as 1 million euros in annual revenues. In addition, this distinction between SMEs and large companies needs to be flexible. There are some excellences in SMEs that have always turned out to be very careful to cybersecurity and for which at the same time the same pricing could not be applied as for other SMEs. For example this is the case of start-ups e.g., Fintech, Insurtech that have what is called *security by design*.

2.3 The case of Cyber Essential

Since the many possible requirements on the part of the insurer/reinsurer and the broker are many, variable and extremely confidential, it has been decided in this section to elaborate on some of the public sector requirements. These are freely available on government sites. This is the case, for example, with the UK government.

The high (often unsustainable) costs for audits of SMEs were discussed in the previous section and also the help that can come from the private sector. Instead, the United Kingdom, has suggested and started to implement a solution that is certainly worth discussing. The British government, through the National Cyber Security Centre (NCSC) devised (almost 7 years ago) a certification[3] called *Cyber Essential* designed especially for small and medium-sized enterprises. It is continuously being improved and, in addition to being funded and supported by the British government, it also increases the reputation of SMEs by providing them with this certification in the cyber sector. Basically it gives training and practical tools to defend against common and uncommon cyber attacks at a low cost, relieving companies from having to support external auditing processes or expensive private consultancy.

The advantages are *undoubted* because first of all, costs are lowered by a great deal. Consider that the cost of the certification starts at about 300

[3] NCSC - Cyber Essentials - `https://www.ncsc.gov.uk/cyberessentials`

pounds for smaller companies and goes up to 4-500 pounds for larger companies. The cost has also remained roughly stable over all these years. It also provides awareness of your company's level of cybersecurity and IT culture. These kinds of certifications could be adopted and imposed by many countries with the purpose of having a multitude of data about the cybersecurity status and how it evolves over time and also could be required (as is already the case in the UK) to collaborate with public institutions. In addition, one could think about requiring them for standard contracts between private entities/individuals as well, so as to try to mitigate the exposure to problems in supply chains and setting a new (higher) standard in the business.

It is good to note that it is not as easy to obtain a certification like the UK one and that therefore these types of certifications are certainly not worthless. The entity gets a lot of help to be compliant, but it has to meet specific requirements. Some examples for the IT infrastructure required by the NCSC can be found in [7] and to sum up they are:

- *Firewalls* for internet connection of all devices for corporate use. In this way it is possible to securely access the SMEs network services. The firewall[4] allows incoming and merged traffic to be monitored using a predefined set of security rules to allow or block events. It can be software or hardware and is considered a company's very first line of defence regarding Internet connections.

- *Secure configurations* - In this case there are a series of prescriptions designed to ensure that every computer and network devices are configured to reduce the level of vulnerability and that they provide the functionalities designed to perform *only* their role. An *ad hoc* example is the company mobile phone which must be configured in such a way as to block the installation of apps that are potentially dangerous and not useful for carrying out work.

- *User access control* - These requirements aim to ensure that each account provided by the company is assigned to authorised individuals

[4] `https://www.cisco.com`

and that you have access to the services and data strictly necessary to carry out your job. For example, an employee who is not involved in accounting should not be able to have access to applications that deal with accounting. Still referring to user access control, it is required to introduce password-based authentication and introduce password access protections. Some examples are multi-factor authentication (MFA) by which codes are generated on enabled applications or devices and require the user to enter, in addition to their credentials, this code. Some additional protection measures may be requirements on the type of password chosen and how often it should be updated. Long, complex passwords and having different ones for each account should always be preferred. Also there may be measures such as locking the account after many consecutive password attempts.

- *Malware protection* - The main objective of this measure is to prevent the execution and/or downloading of known malware and also "untrusted software." In practice it is implemented by preventing the installation of any application upon approval of the IT department or a manager. Unfortunately, the damage from malware that has infected a device can be identified a very long time later, and by that time it may be too late to limit the damage. Many can also be restrictions and filters for email attachments and anti-malware software that offer automatic scanning of all documents that may affect an employee during his or her work.

- *Security update management* - It means that it should not be tolerable for a company (large or small) to be a victim of a vulnerability that is known and would have been avoidable simply by updating software applications. This is why it is always important to have the latest updated version of all applications that are used and to install them in a timely manner as soon as the opportunity arises.

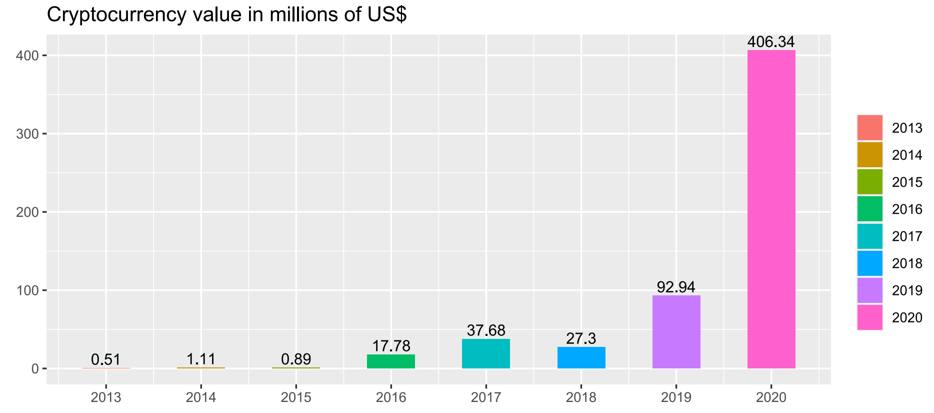
Additional advice that is imposed in order to become certified is to always make periodic backups of your data. Having a backup that you can rely on and that is recent can really make a difference in an emergency and after you have been attacked. It can allow you to quickly reestablish an entity's activity and allows you not to lose data, even if the original data is encrypted and cannot be recovered. As you can easily see these requirements are only a starting point for good cyber *resilience*, but they require numerous actions and investments in IT and training to be applied all of them.

2.4 The situation in Italy

This section will present a portrait of the state of cybersecurity in Italy and what the most common risks are. An attempt will also be made to describe and contextualise them to the current situation in Italy.

It is unavoidable to talk about the situation in Italy without referring to the Clusit Report [9], which for many years now has been publishing its analyses and refining them for the Italian landscape. It is a report compiled by numerous IT professionals with expertise in the field and brings together information received from open and non-open sources. Even in its latest version it presented a situation that was noticeably *worse* than the year before. The peculiarity of cyber risk is that each year the range of risk sectors and types of attacks discovered and yet to be classified seems to widen. To better describe this concept it can be recalled that in 2011 Clusit itself had spoken of 2011 as the *Annus Horribilis* of cyber security in Italy. Since then things have only gotten worse.

It is worth remembering that until not too many years ago, the World Economic Forum itself did not report cyber risks as a major risk worthy of special attention in the *Global Risk Report*. They were officially included in the reports only starting in 2015 and since then the attention paid to them has been steadily increasing until they are (already in 2019 i.e. 4 years later) ranked first in terms of impact and likelihood of occurrence. Such a rapid rise in the rankings can be easily explained by graphs like the one in the Figure 2.3. It shows the total value in cryptocurrency (mainly Bitcoin) that has been received by those who have perpetuated a ransomware-type attack. It is good to remember that these amounts are largely underestimated estimates since only a small fraction of all payments are known



Data source: Chainanalysis - "Ransomware 2021: Critical Mid-Year Update"

Figure 2.3: Total Cryptocurrency Value Received by Ransomware Addresses, 2013-2020

from open sources. In addition, there are all those types of attacks that do not have ransomware as their goal, but rather the theft of sensitive information, either to resell it on the *dark web* or to appropriate industrial patents.

What is certainly striking about the Figure 2.3 is that, when referring to a cyber claim, the ransomware payment is only a fraction of the total cost of the claim. Mainly, the insurer has to compensate for business interruption, provide assistance to the company that is the victim of the attack, pay consulting firms to deal with the perpetrators of the attack, and possibly also damages to third parties produced by possible privacy damage and data dissemination. What happens in fact is that victims are often faced with *double extortion*, that is, a threat to disseminate the stolen data if they do not pay the ransom in addition to the primary threat of not sharing encryption keys in the event that company data has been encrypted.

The sources analysed by the Clusit Report show about 2,049 attacks occurring globally (including Italy). Considering that all those classified since the Report has existed are 14,000, of these as many as 7,144 (approximately 50%) have occurred in the last 4 years. The other data source analysed by the Report is provided by Fastweb[5], which, thanks to their *Se-*

[5] `https://fastweb.it/corporate/?lng=EN`

curity Operation Center (SOC), made it possible to identify in 2021 alone *42 million* "security events" against 6.5 million public IP addresses managed by Fastweb itself. The increase in the number of security events from 2020 to 2021 was 16%. The detected security events were obtained by combining those proceeds from the SOC, but also from other sources such as national and international Computer Emergency Response Teams (CERTs) and data from external organizations such as the Shadowserver Foundation.

Classification of attacks. The possible types of attacks are many, and each of them has many sub-categories. Combining the categories used by ENISA's *Open Threat Taxonomy* ([10], [11]) analysis, the *Open Threat Taxonomy*[6] and other international frameworks, the Clusit Report (focusing on the Italian sector) identifies the following macro-categories:

- *Malware*. This term refers to all possible software, firmware, or code that has been created with the intention of executing an unauthorised process for malicious purposes. The impact of this process must be adverse and must affect the confidentiality, integrity, and availability of a system. Within this category is, for example, the first *worm* ever created. The idea of the worm, that is, a self-replicating program that is capable of infecting another computer, was born in the mid-1950s by mathematician John von Newman, who was the first to theorise and propose the possibility of self-replicating programs in [20]. Other examples of malware are *trojan horses* and all that malicious code that aims to undermine the integrity of a system. *Spyware* and *adware* also fall into the general category of malware. The latter is a kind of advertising malware used primarily for commercial purposes and extremely widespread.

- *Vulnerabilities*. They are components of a computer system for which no (or very little) security measures are in place. They are, in essence, real weak points that can be exploited by malicious attackers. The ENISA Report of 2022 ([11]), for instance, noted, on a European level,

[6] https://www.auditscripts.com/free-resources/open-threat-taxonomy/

a consistent increase in exploitations of *0-day* and other critical vulnerabilities. The problem of vulnerabilities is not a trivial one, as the increasing number of software solutions for every sphere of everyday life means that the number of vulnerabilities and consequent opportunities for malicious attackers increases. There is also a real market for vulnerabilities, especially so-called 0-day vulnerabilities. These are software vulnerabilities that are not known to the developers of the software itself and, even if they are known to the developers, are not handled. Thanks to this flourishing (unofficial) market, it is possible to buy *0-day malwares* that have the advantage of being disruptive, unexpected and, from a technical point of view, do not leave their *signatures*. The signature is a sequence of bytes and information common to families of malware.

- *Phishing/Social Engineering*. This type of attack includes all those actions carried out by malicious persons with the aim of exploiting a human error or human behaviour in order to obtain something in return. This type of attack is very sneaky because it bypasses all software and hardware barriers. There are many ways to perpetuate this type of attack. One can act, for instance, by manipulating the other party through well-constructed e-mails that try to adapt to the company and the person they are addressing. For instance, there are versions of phishing/social engineering emails that are able to automatically insert the logo of the company they are addressing. Victims who have been manipulated may consequently reveal sensitive information, provide access codes, bank account information, provide documents or facilitate the installation of further malicious software in their organisation's computer systems.

- *Identity Theft/Account Cracking*. In this type of attack, which is primarily in the macro-category of *threats against data*, there is identity theft through which an attacker uses *Personal Identifiable Information* (PII) to impersonate a user. An example would be the theft of credit card credentials with the aim of making unauthorised expenditures by the legitimate owner and lowering his or her creditworthiness.

The macro category refers to the set of threats whose primary objective is to gain access to and disclose data sources. The information to perpetuate identity theft can be found through *data breaches* (intentional attacks by cyber criminals) or *data leaks* (events causing unintentional release of sensitive, confidential and protected data). There are also cases of *syntetic identity theft* through which a cybercriminal combines real and fictitious data with the aim of creating a new identity. The theft of personal information can be extremely lucrative. It should also be emphasised that a single U.S. medical record can be sold on the dark web in the range of 50 to 1,000 U.S. dollars.

- *Web Attack*. This classification is used by to collect all other possible attacks on network resources. For example, there is the *cross-site scripting attack*, which is a vulnerability in a website that allows scritps (e.g. JavaScript) to be inserted into it that can be exploited maliciously to the point of even taking control of the user's computer. Then there are other attacks such as the *SQL injection attack* that allows malicious SQL scripts to be inserted on a web application. The purpose is to gain access to the data stored on that server. Once full control of the server's data is taken, it is possible to copy, modify, and even delete it. Another possible attack is the so-called brute force attack by which an attacker tries to guess usernames and passwords for access to a corporate login or on a website simply by attempting every possible combination of letters, numbers and alphanumeric codes. There are software programs that either search using the most common passwords or have special glossaries that, combined with personal information found on the user, can allow them to guess login credentials. Today it is no longer so difficult to think of a brute force attack since it is possible for hackers to have access to multiple computers and cloud computing to increase computing power.

- *DDoS* stands for *Distributed Denial of Service* and is an attack technique that allows in causing a malfunction of a website or service by saturating its resources and thus preventing it from delivering the service. The attack is very difficult to stop quickly because it comes from a multitude of systems, so it is not enough to block one source to stop it. This type can be placed in the macro-category of *Threats against availability*. DDoS are getting larger and more complex and they are moving toward mobile networks. Unfortunately, there is a real market for buying and selling these DDoS services and the *barriers to entry* are lowering year by year, allowing even inexperienced and/or low-skilled cybercriminals to conduct sophisticated attacks. These attacks usually do not last very long if they are promptly blocked. However, they can cause disruption to end users that are prevented from accessing, for example, a hospital or government agency website. Usually, in the most severe cases, a ransom is also demanded to restore the system to proper operation.

- *Multiple Techniques*. This category includes all those attacks that use a mix of other attacks. The goal is to maximise the probability of success of the malicious operation and make the ransom demand more credible as well as cause the greatest possible loss.

As can be seen in Figure 2.4 and Figure 2.5, the attack category that has the largest numbers is malware. For example, in 2021 it reached 41.48% of Fastweb's registered attacks, an increase of 9.7% over the previous year. The unknown category is also important in absolute number of recorded events and as a percentage increase over 2020. It is in fact an increase of 16.4%. Classified as unknown are all those cases in which one becomes aware ex post of a data breach or data leak perhaps on the deep web, but is unable to reconstruct the type of attack of which that undertaking was a victim. A decrease in Phishing/Social Engineering cases is also reported (-32.1%). However, this should not be too reassuring because a decrease in mass phishing cases has been noted in recent years, but at the same time an increase in the sophistication of the attacks and the effort expended to bring them to completion. There is a growing awareness on the part of attackers that it is better to invest resources in a well-crafted phishing campaign than to try to focus on the quantity of attack attempts.

The other relevant attack type that marks +60% over 2020 is attacks that exploit the existence of vulnerabilities. Alone, the malware and vul-

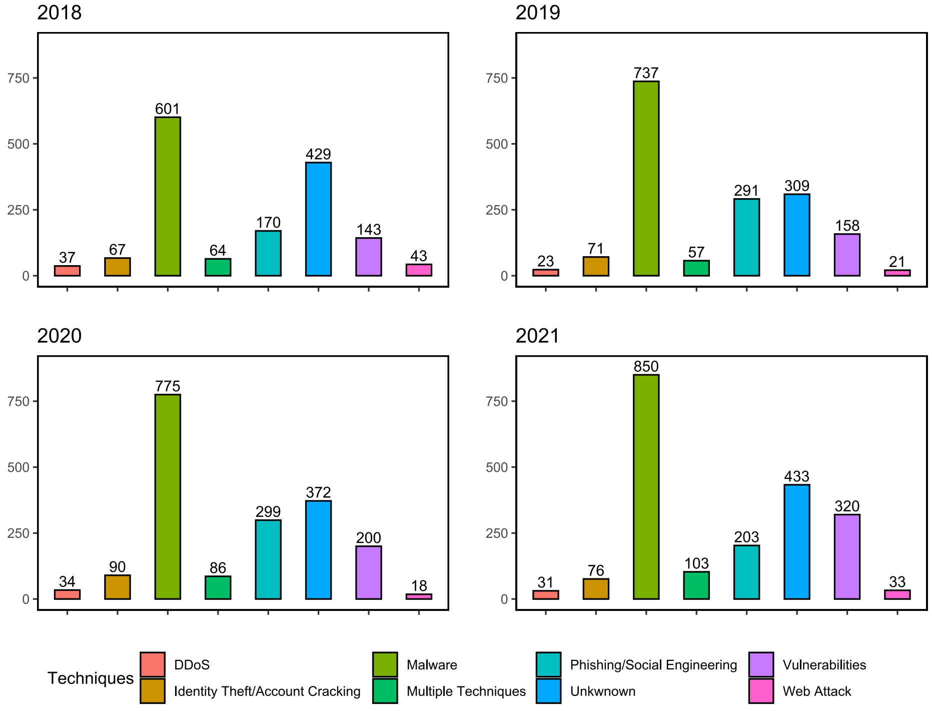


Figure 2.4: Attack techniques from 2018 to 2021

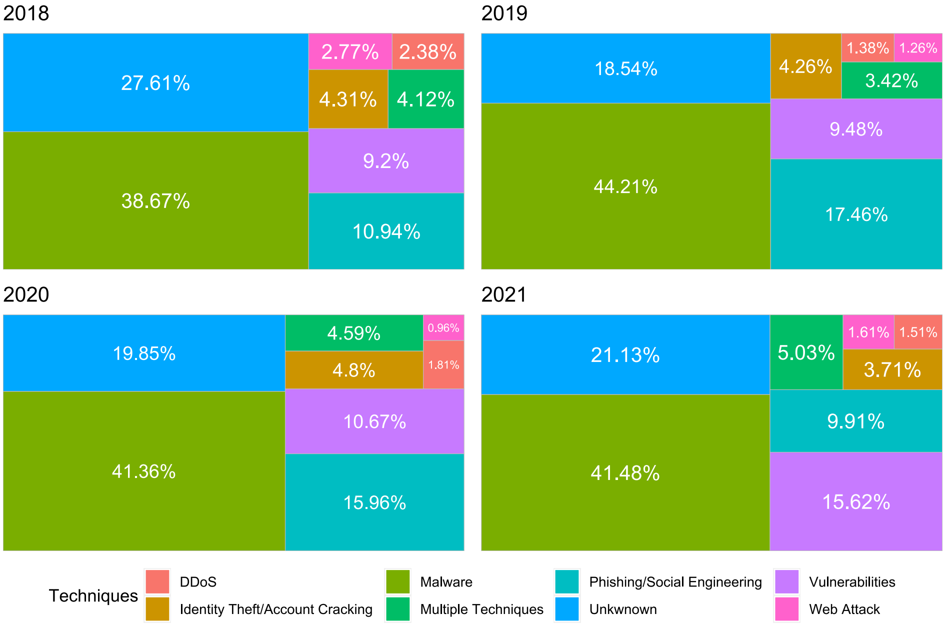


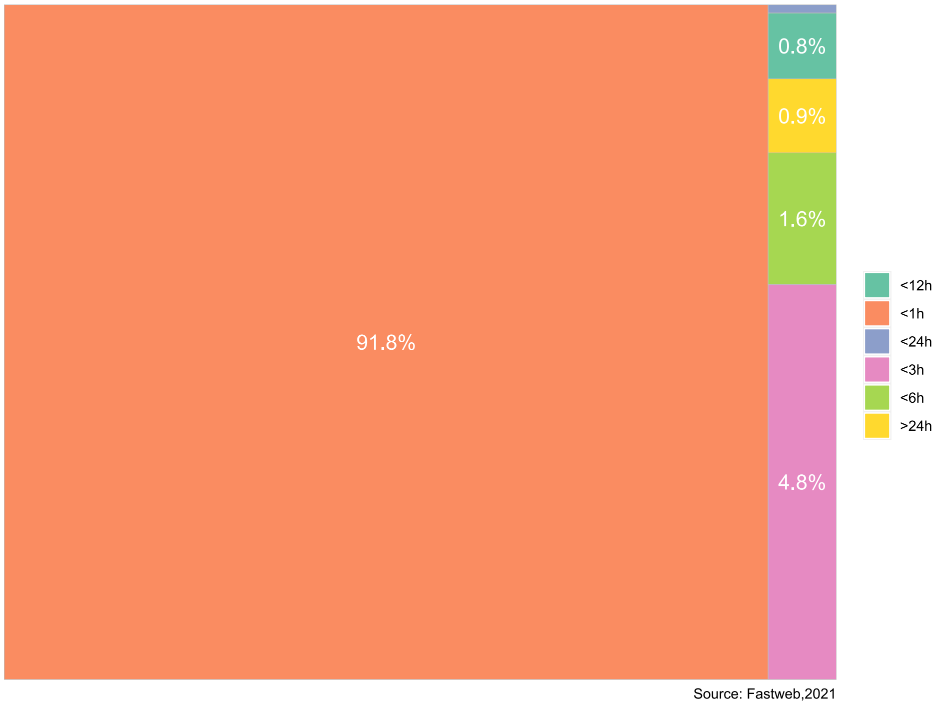
Figure 2.5: Percentages of attack techniques from 2018 to 2021

nerabilities category made up 57% of attacks in 2021 according to the sources analysed. In the data analysed in Italy by Fastweb, the relevance of the malware category is even greater, marking a net +58% over the previous year. The most prevalent malware is from Andromeda, which is a platform that allows you to buy (in a modular way) up to 80 families of malware. The modular nature of Andromeda and the extreme ease of use by malicious attackers make it possible to lower the cost of barriers to entry and calibrate the type of attack to suit one's needs. Another type of malware that is widely used in Italy is Downadup. This is a worm that manages to exploit unpatched Windows network vulnerabilities and easily enters the list of malware that has infected the most devices in history.

According to [9], the most affected sectors in Italy are Finance/Insurance and Public Administration, which together make up 50% of the cases in the last survey period. It should be noted that public administration is of particular interest because it contains a great deal of sensitive data (such as health data) and also often lacks adequate IT protections as well as cyber policies. In third place as the most affected sector is the more general Industry sector, which accounted for 18% of attacks in 2021.

An increasing presence of viruses going to attack mobile devices was also noted in Italy. This is usually done through *smishing*. The latter is the so-called sms phishing i.e., a form of phishing that aims to request personal information and/or sensitive data through text messages on the victim's cell phone. Some research, including a research conducted by Gartner[7] shows that up to 98% of users view a phishing sms and even 46% respond to it. This phishing technique is particularly used because people respond much more easily to a text message than to their email and place greater trust in it. Secondly, for sms, all the more advanced spam filters that are present for email inboxes are not often present. Finding a potential victim's cell phone number is also easier than finding their personal email. For example in the case of a mass-attack it will be sufficient to attempt all possible combinations of 10 numbers and is much simpler than attempting combinations of all the non-standard-length alphanumeric codes in an

[7] https://www.gartner.com/en



Source: Fastweb,2021

Figure 2.6: Detected duration of attacks using DDoS type.

email.

DDoS attacks are also becoming increasingly common in Italy. In 2021, about 2,500 events and more than 18,000 anomalies attributable to possible DDoS attacks directed at Fastweb customers were detected. Unfortunately, the barriers to entry for this type of attack are really low. For a 5-10 minute attack with 100Gbps of traffic generated on the website, 5-10 USD dollars are required with a subscription service. In Italy the average duration of 97% of these attacks is less than three hours.

The distribution of attack duration can be seen in Figure 2.6. Only a small percentage of attacks have a duration longer than 24 hours (0.9%). DDoS attacks are often carried out through so-called botnets. These are a collection of devices from various agents (often completely unaware of this usage) that have been previously infected to make mass traffic to an Internet page or online service.

Threat Motivations There may be many reasons for the threats, but in Italy and Europe more generally, ENISA ([11]) traces them to the following:

- *monetisation* i.e. any financial related action carried out by malicious actors. this is the case, for example, with ransom payments.
- *geopolitics/espionage* i.e. any action aimed at taking possession of intellectual property or confidential/sensitive/classified data. Usually these types of attacks are carried out by states by means of hacker groups acting to hide the main mandate. An example of such an attack was carried out successfully by a group backed by the Russian government in 2020. Numerous public agencies in America (e.g., the Justice Department, Centers for Disease Control and Prevention) and in countries such as UK and Europe (e.g., NATO, European Parliament, UK National Health Service) have confirmed that they have been victims of this attack.
- *geopolitics/disruptions*. The goal in this case is to carry out destructive actions in the name of geopolitical principles.
- *ideological*. In this case one finds all those attacks moved by ideological motives such as hacktivism.

2.5 Solvency II and operational risks in a nutshell

Section 2.1 gave a comprehensive definition of Cyber Risk and described it primarily as an operational risk. In the case of insurance and reinsurance institutions, however, it has a dual significance. It can either be an operational risk or a *non-life underwriting risk*, since the insurance/reinsurance undertaking may sell cyber policies and thus be subject to pricing, reserve, catastrophe risk or it may itself be the victim of a cyber attack. It is important to remember that insurance companies are considered systemic entities from an economic and social point of view and possess large amounts of confidential data and information that could cause reputational damage to the entire industry and its policyholders. This is the case, for instance, with the sharing of clinical data and confidential information.

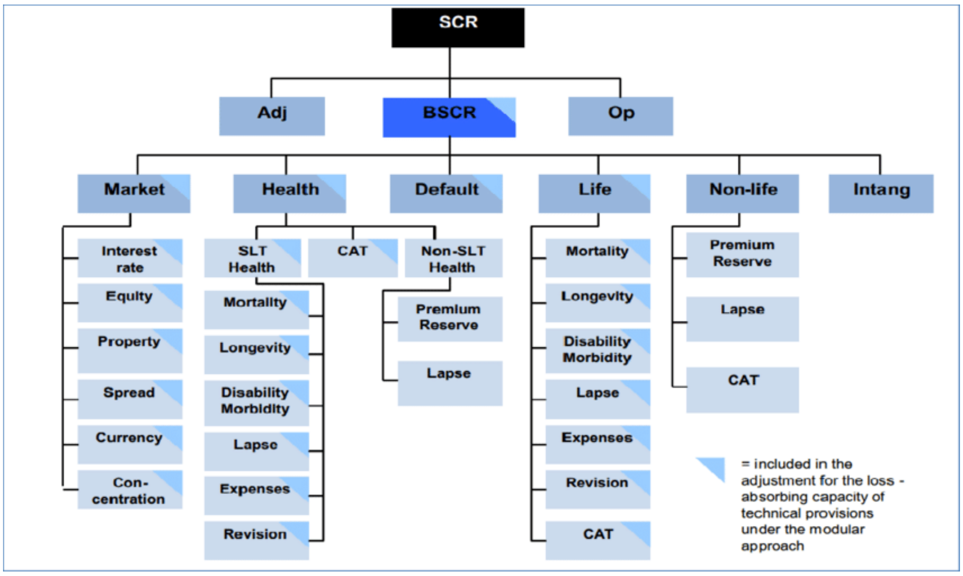
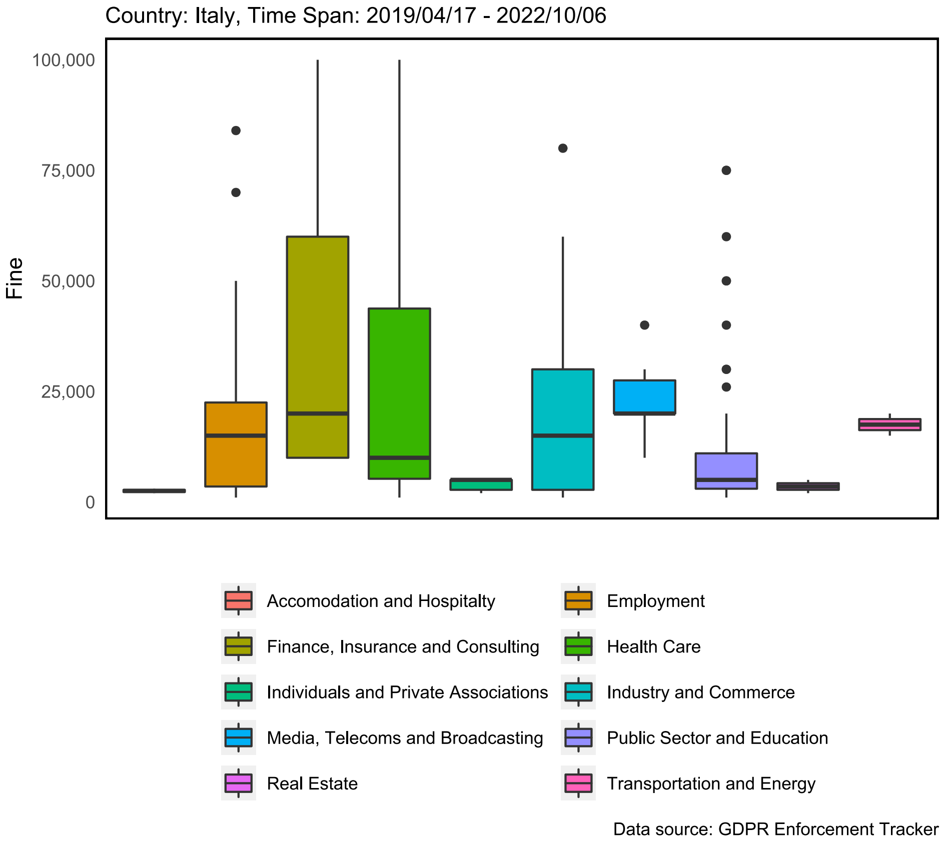


Figure 2.7: Solvency II Standard formula structure.

Cyber (operational) risk In Directive 138/2009/EC (Solvency II directive), this dual point of view is addressed also in the standard formula and the SCR capital requirement needed to be solvent with a one-year horizon at 99.5%. According to the Solvency II directive, the operational risk module must include all risks of loss resulting from inadequate or failed processes, human resources and systems, or from external events (e.g. cyber risk). Operational risks also include the risk of non-compliance (*compliance risk*) and the risk of incorrect representation of items in the financial statements. Compliance risk is closely linked to cyber risk and from the point of view of personal data and after the introduction of the European GDPR privacy directive is not at all relevant. In the Figure 2.8 and Figure 2.9, one can see and example of the distribution of fines by the privacy watchdog (Garante della Privacy) to different sectors in Italy between April 2019 and October 2022. As can be seen, the variability of the amount of fines can be significant, especially in some sectors. In the reporting period there were fines to financial and insurance institutions for insufficient fulfilment of data subjects rights, for non-compliance with general data processing principles, for insufficient legal basis for data processing etc.

Cyber risk from an operational risk perspective can be approached with



Data source: GDPR Enforcement Tracker

Figure 2.8: Boxplots of different sectors for fines of less than 100,000 euro

different approaches depending, for instance, on whether the company uses a standard model or an internal model. Taking the example of a company that uses the internal model (such as Generali Assicurazioni S.P.A.) one can read in the Solvency and Financial Condition Report of 2021 ([24]) that cyber risk is confirmed to be among the most relevant risks for the company. The company reports that it has set up specialised units within the first line of defence in order to deal with this specific risk and these units act as key partners for the Risk Management Function (one of the four fundamental functions established with the entry into force of Solvency II, together with the Actuarial Function, Compliance Function and Audit Function). Using an internal model, Generali Assicurazioni S.P.A. calculates the capital requirement for operational risk by asking the heads

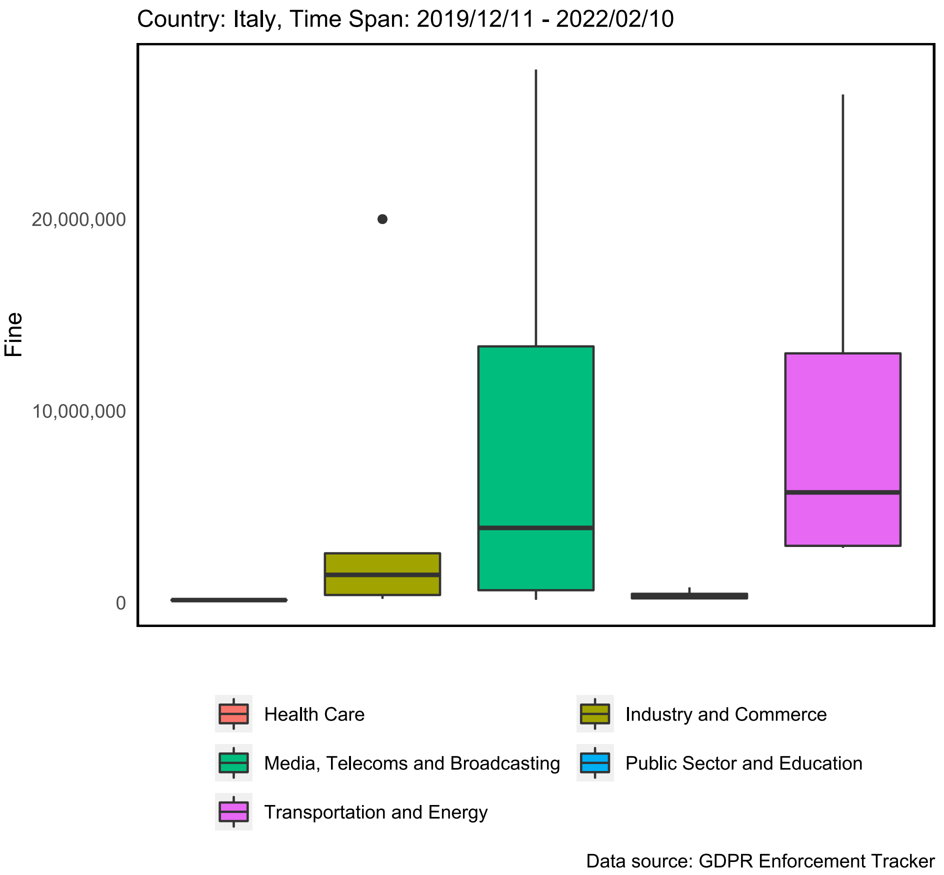


Figure 2.9: Boxplots of different sectors for fines greater than 100,000 euro

of operational areas for frequency and impact estimates for each operational risk category. These data are used to calibrate the internal model. In this way it is possible to obtain probability distributions of losses over a 12-month time horizon. Subsequently, the losses are aggregated to obtain the overall annual loss distribution and consequently the overall capital requirement for operational risk (and thus also for cyber risk).

Basel II and Solvency II have provided frameworks (now well established in the insurance landscape) for operational risk. [3] and [2] have drawn on this operational risk framework to illustrate cyber risk in more detail. In [6] 4 categories of cyber risk were identified:

- *people actions* - They can be inadvertent, deliberate, or due to inaction.

In the first case there are all unilateral actions that are taken without malicious or harmful intent. For example, errors and omissions fall into this category. Actions can then be deliberate and thus aimed at intentionally causing harm to property or persons. Then there are inactions that occur because of a lack of action at the appropriate time or in a failure to act in a given situation. A prime example is the case of lack of appropriate skills or lack of proper knowledge.

- *systems and technology failures* - This includes hardware, software and systems more generally. In the first case you have the risks that can be traced to damage to physical equipment. This is the case, for example, of obsolescence of electronic equipment. In the second case you have risks due to lack of software of any kind. We then refer to business applications and their security and appropriate use updates. In the last case you have the failure of integrated systems that have failed to perform as expected, probably due to design, their integration or intrinsic complexity.

- *failed internal processes* - In this case there is the case of "design and/or execution" of something. it is the case, for example, of wrong allocation of roles and responsibilities within the company or wrong process flows and escalation of issues. Then there are the cases of process controls and supporting processes. The former occurs when there are inadequate controls in the operations of a process.In fact, every process in the company should be carefully monitored by checking its KPIs, status and provide for periodic reviews. The second, on the other hand, occurs, for example, when there is wrong training or wrong procurement i.e., whenever there is a failure to bring in the necessary resources.

- *external events* - This category includes all those actions that are exogenous to the company under consideration. There can be, for example, various types of disasters (man made or natural). Then there can be legal issues such as a sudden change in legislation or litigation. Then there can be business issues such as in the case of adverse market conditions or economic conditions. That is, all those adverse conditions that have occurred in the organisation's environment. Lastly, there are service dependencies that occur when there are relationships with third parties, such as utilities, emergency services, consulting, etc.

In [3] there was an examination of data in the SAS OpRisk Global Data source that collects 22,075 incidents involving operational losses over approximately 40 years (up to 2009). Mostly these are incidents collected and categorised according to the Basel II framework, but one can still get valuable considerations for the insurance business. The goal of the analysis was to be able to find a *complete cost* of an operational risk event with direct and indirect effects, keeping reputational losses aside. Of all the incidents involving operational risks in general, 994 were related to cyber risk incidents. Some basic statistics such as mean, standard deviation, minimum/maximum, empirical quantiles, and some risk measures such as Value-at-Risk (VaR) and Tail Value-at-Risk (TVaR) were analysed in the database used. These data were calculated for cyber and non-cyber incidents and also for the 4 categories explained above. The data collected indicated a significantly *lower* average cyber risk losses than non-cyber risk losses ($40.53 mln vs $99.65 mln.). The standard deviation was also significantly lower (443.88 vs. 1,169.17). Regarding the risk measures, the VaR and TVaR of cyber risks turned out to be smaller than those of non-cyber risks and also regarding extreme cases (maximum losses) cyber risk was around $13,313 mln while non-cyber risk $89,143 mln. Regarding the 4 categories, on the other hand, the analysis had shown (cyber) operational risk to be more likely for "actions of people" and less likely for "external events".

Referring also to the empirical distribution of losses by cyber risk and non-cyber risk, many differences were found. The latter has a much heavier tail than the former and this could be explained by significantly higher absolute recorded losses. It may be dangerous, however, to generalise this observation even nowadays because the amount of digitisation and computerisation in society is growing year by year and with it the possible attack surfaces. In Solvency II, however, these results can certainly be used to model cyber risk differently from other operational risks and then aggregate and make appropriate diversifications from a capital requirement perspective. Also from the perspective of cyber (operational) risk, it had been found that there was a marked distinction between companies that financial and non-financial. In the former case the average loss was significantly higher for cyber risk. While in the second case the average loss was higher for non-cyber risk. It is noteworthy that in the data collected by SAS, 78.6 percent of all cyber incidents had occurred in financial institutions. The trend today is a widening of targets by malicious actors, thanks in part to the resilience of financial and insurance institutions.

The point of view of the underwriter Insurance companies, as noted above, also address cyber risk from the perspective of the policy underwriter and undertaking that is responsible for writing cyber policies, managing their reserves and selling them in the market. This exposes them to risks such as underwriting, reserving, and catastrophe risks that may also be cyber in nature. The main challenges from an underwriting perspective are those of the extreme difference that each potential policyholder makes to the others. IT systems can be as diverse as hardware equipment and its use. The degree of computerisation in the company, the web presence, the type of data processed etc. may be different, and this imposes a high degree of customisation of the policy on the insurer.

The main problem, however, is the scarcity of available data, which are often absolutely lacking or grossly inadequate for accurate actuarial calibration and to allow any models to be tested. Indeed, it is known from the statistical literature that to possess a good model one must have data on which to test it as well, and the data should come from a rigorous and reliable test set on which the model has not been calibrated.

Dealing with this lack of reliable information, insurers are forced to operate under uncertainty and be more conservative. This results in low maximum coverages and high deductibles for example. On the policyholder side, however, cyber coverage that is not perceived as "true" coverage loses interest and does not add value to what is already being done by risk management in the corporation. Still referring to the underwriter's point of view, there is also the problem of the variability of cyber risk and consequently the difficulty of obtaining a sufficiently long time series. Also not to be underestimated are the regulatory risks. What is required from the regulator is as precise and step-by-step guidance as possible, while on many issues (such as the possible indemnification of ransom payment by the insurance company) there are too many legislative uncertainties and individual courts could overturn what the underwriters anticipate.

Another problem faced by underwriters and from a pricing perspective is adverse selection risk. Using assessment questionnaires too lightly to simplify the underwriting process could lead to adverse selection, and this should be avoided as much as possible, taking into account the inherent difficulty of this type of business. What would be advisable is a sharing of at least best practices among underwriters, insurers and reinsurers for dealing with cyber risk.

2.6 Silent Cyber Covers

One aspect to be taken into account in the insurance business is the phenomenon of *silent* cyber covers. This is due to the substantial difference that exists between so-called affirmative and non-affirmative policies. Indeed, as [1] mentioned, affirmative policies are those policies that explicitly list the risks covered and/or exclude those not covered. Non-affirmative policies are the all risks, as they have a different and varied scope and range of cover. In the area of cyber risks, non-affirmative policies are particularly dangerous and are also called "silent" policies, this is because an insurer may have inadvertently issued a property policy that *also* covers cyber damage (physical and non-physical).

Issuing policies that might also cover losses not foreseen at the time the policy was priced exposes the insurer to a very large risk, since the policies have already been issued and therefore no exclusions can be made retrospectively. It may also be very difficult to prove specific exclusions in litigation. Think of cyber attacks carried out by hackers and encouraged/financed by a third country. It may be very difficult to trace the attack back to a war matrix, and consequently the insurer may not be able to deflect from paying the claim.

For this reason, insurers and, more specifically, underwriters should move towards affirmative property policies to develop *ad-hoc* covers for cyber risks and be as precise as possible in listing what can be covered by the policy and what cannot.

Chapter 3

A proposal for a one-year contract

In this chapter, some more or less common methods for pricing cyber policies will be presented and one of them in particular will be explored. Although cyber policies are beginning to gain a certain amount of interest, especially in the US, the pricing methodologies are not so straightforward and are difficult to compare since they are usually developed for policies covering third-party damage, assistance, etc. These policies can then be more or less standardised and the calibration (given a certain theoretical model) depends on many factors.

3.1 Review of cyber risk models

In [16] and in [28] it is possible to find a review of the state of the art of modelling and pricing cyber insurance. As will be seen in the following discussion, these methods can be very different from one another, although they do have some common features.

Historically, from an actuarial perspective, in order to price an insurance product to cover a certain type of risk, models and underlying distributions have always been sought to try to describe the loss. The objective was to identify an expected loss and, by adding safety loadings and other loadings such as expense loadings (and taxes) to find an insurance premium. From a risk management perspective, the objective is to identify risk measures such as VaR (Value-at-Risk) or TVaR (Tail Value-at-Risk) with the aim of analysing tail events, also called worst case scenarios.

In classical actuarial mathematics, there are two distinct approaches to representing the aggregate cost variable of claims (e.g. cyber losses) over a given period of time. It should be borne in mind that usually the reference period is one year since these are non-life contracts, but in certain cases it could be of a different duration. The first approach is called the *individual approach* because, given a portfolio of N heterogeneous risks, $\tilde{Y}$ is the cost of claims for the individual insured risk. The classical assumptions of this model show a number of insured risks that is not a random variable, on the contrary, it is known at inception of the contract and the variables represented by $\tilde{Y_1}, \ldots, \tilde{Y_N}$ are usually independent of the number of claims that generated it.

$$\tilde{X} = \sum_{\ell=1}^{N} \tilde{Y_\ell} \tag{3.1}$$

This approach obviously involves realisations of $\tilde{Y}$ which may be zero in a year and which may also represent the sum of a random number of accidents during the insurance coverage period. Consider the case of motor TPL where it is entirely possible to cause more than one accident during the year. If one assumes independence of the $\tilde{Y}$ variables over the year, one can derive the aggregate claims cost distribution function by *convolution* of the independent and identically distributed $\tilde{Y}$ random variables. Consequently, it can be shown that, given the same assumptions, the expected value of the aggregate claims cost is equal to the sum of the expected values of the individual random variables Y and also the variance. A similar relationship exists for the skewness of the aggregate claims cost.

$$\mathbb{E}(\tilde{X}) = \sum_{\ell=1}^{N} \mathbb{E}(\tilde{Y}_\ell) \tag{3.2}$$

$$\sigma^2(\tilde{X}) = \sum_{\ell=1}^{N} \sigma^2(\tilde{Y}_\ell) \tag{3.3}$$

$$\gamma(\tilde{X}) = \frac{\sum_{\ell=1}^{N} \mu_3(\tilde{Y}_\ell)}{\sigma^3(\tilde{X})} \tag{3.4}$$

Where μ_3 is the central third moment, defined as $\mu_3 = \mathbb{E}(\tilde{X} - \mathbb{E}(\tilde{X}))^3$.

The second 'classical' model is called the *collective risk model* or also the *frequency severity* approach. It is widely used in many classes of business, and uses of this model are also known in the cyber insurance business. Unlike the previous approach, this one is based on two types of random variables, namely the number of claims $\tilde{K}$ generated by the contracts in the observation period (e.g. 1 year) and the cost $\tilde{Z}$ generated by each claim. The aggregate cost of the claims will be given by a compound process in which the above random variables interact:

$$\tilde{X} = \sum_{\ell=1}^{\tilde{K}} \tilde{Z}_\ell \tag{3.5}$$

This approach offers a change of perspective from the individual approach as it allows the entire portfolio to be modelled directly and not each individual policy. The number of random variables to be dealt with will therefore be smaller. The classic assumptions are as follows:

- Claims always occur at arrival times in the observation period between 0 and t and the random variable $\tilde{K}$, at distinct time instants, can be considered (from a probabilistic point of view) as a *counting process*;

- Independence is assumed between the number of claims and the random variables $\tilde{Z}_\ell$;

- Independence and identical distribution is assumed for the random variables cost of claims $\tilde{Z}_\ell$.

These assumptions allow the aggregate claims cost distribution function to be defined as:

$$F_{\tilde{X}}(x) = \mathcal{P}(\tilde{X} \leq x) = \sum_{k=0}^{\infty} \mathcal{P}(\tilde{K} = k) \cdot \mathcal{P}\left(\sum_{\ell=1}^{k} \tilde{Z}_\ell \leq x\right) \tag{3.6}$$

An alternative version involves the use of the convolution of order k of the variables $\tilde{Z}_\ell$ obtaining:

$$F_{\tilde{X}}(x) = \sum_{k=0}^{\infty} \mathcal{P}(\tilde{K} = k) \cdot F_{\tilde{Z}}^{k}(x) \tag{3.7}$$

Usually these assumptions can be verified, but the matter becomes more complex when referring to cyber insurance. The first problem is caused by the lack of statistical data and their number and quality. The calibration of actuarial models (even simple ones) is inseparable from accurate data quality and granularity. There are commercially available databases of cyber data from open sources or insurance companies/brokers but the main problem is usually the quality of the data. It is not uncommon, for instance, to have to discard most of the data purchased due to a lack of complementary information. In this regard, one can refer to [18] where one can see that, in order to apply their model, the authors gets $130,000$ cyber risk events from the data provider Advisen and 97.4% of the observations are removed. The reasons are incomplete information on monetary losses, lack of accurate information on the company, the company sector, etc.

The second reason why the collective risk model struggles with cyber insurance is that cyber technologies and threats evolve very, very quickly. Unfortunately, this does not only undermine the *underwriting process* (of primary interest in this discussion) but also the *reserving process*, *operational risk assessment* and *reinsurance*. The accuracy of historical data and past claims becomes almost futile compared to the speed of change and adaptation of the threat itself.

The third reason is that a cyber incident hardly affects one policyholder at a time. From this point of view, risk independence can no longer be assumed. Exacerbating this picture is the fact that, unlike meteorological/seismic phenomena and more generally natural disasters, cyber threats do not have a well-defined geographical/physical delimitation. While it is true that in the event of war (e.g. the situation in Ukraine) there may be a greater number of cyber attacks from (and towards) a particular country, it is also true that a virus can spread uncontrollably across several states and even entire continents, given also the globalisation in the society.

The modelling of cyber risks according to [16] falls into 3 broad categories. Models for *idiosyncratic* risks, models for *systematic* risks and models for *systemic* risks.

Idiosyncratic risks are those risks that may affect a single policyholder independently of all other policyholders. These risks are specific and have a particular target as a target. Models dealing with these types of risks are targeted on the characteristics of the entity under consideration. Systematic risks, on the other hand, are risks resulting from common vulnerabilities among policyholders that may be determined by the use of the same technological equipment, computer systems, etc. In this case, there are therefore common factors.

The objective of this dissertation is instead the modelling of systemic risks, i.e. risks resulting from being part of a network.

An example of a frequency severity method To implement the frequency severity method in the context of cyber risk, an insurance company can start by considering a hypothetical portfolio of n policyholders exposed to cyber risk (usually companies). These companies belong to different sectors such as banking, pharmaceuticals, engineering, services, etc. and may have several variables in common. These variables obtained by means of questionnaires and/or from policy interviews are used to group the companies into G homogeneous groups. Consequently, we have that n_g is the numerosity of group g. It goes without saying that $n_1 + n_2 + \cdots + n_G = n$. These groups make it actuarially possible to adopt the same tariff within the group. The types of cyber threats are divided into C categories. Examples are fraud, data breaches, malware, etc. The aim is therefore to model a frequency severity model *for each* pair (c, g) where g is the g-th group and c is the c-th risk category. It goes without saying that the size of the homogeneous groups and the granularity of the types of threats companies are subjected to influence the accuracy and feasibility of the chosen model. Too high granularity would in fact lead to having very few statistical observations available and to losing underlying statistical robustness.

Given a company i in a group g and with a well-defined risk category c, the following frequency severity model can be considered:

$$\tilde{X}_t^{g,i} = \sum_{\ell=1}^{\tilde{K}_t^{g,i}} \tilde{Z}_\ell^{g,i} \tag{3.8}$$

where $\tilde{X}_t^{g,i}$ is the total aggregate cost of claims up to time instant t (e.g. 1 year) for firm i in homogeneous group g, $\tilde{K}_t^{g,i}$ is the random variable number of claims and $\tilde{Z}_\ell^{g,i}$ $\forall \ell \geq 0$ are the random variables cost of claims for the same firm. The assumptions are the classical actuarial assumptions for the collective risk model i.e. independence of the number of claims and claims severity and independence and identical distributions of the claims severity variables.

This dissertation is not intended to explain the collective risk model applied to cyber insurance in detail, but it may be of general interest to mention that it is possible to obtain information on the mean, variance and moment-generating function of the aggregate cost variable of claims $\tilde{X}_t^{g,i}$ per pair (c, g) even without making further assumptions on the frequency and severity distributions of the claims.

$$\begin{aligned}
\mathbb{E}(\tilde{X}_t^{g,i}) &= \mathbb{E}\left[\mathbb{E}\left(\sum_{\ell=1}^{K_t^{g,i}} \tilde{Z}_\ell^{g,i} | \tilde{K}_t^{g,i} = K_t^{g,i}\right) = \mathbb{E}\left(K_t^{g,i} \cdot \mathbb{E}(\tilde{Z}^{g,i})\right)\right] && (3.9)\\
&= \mathbb{E}(\tilde{K}_t^{g,i}) \cdot \mathbb{E}(\tilde{Z}^{g,i}) && (3.10)
\end{aligned}$$

$$\begin{aligned}
\mathbb{E}[(\tilde{X}_t^{g,i})^2] &= \mathbb{E}\left[\mathbb{E}\left(\left(\sum_{\ell=1}^{K_t^{g,i}} \tilde{Z}_\ell^{g,i}\right)^2 | \tilde{K}_t^{g,i} = K_t^{g,i}\right)\right] && (3.11)\\
&= \mathbb{E}\left[\mathbb{E}\left(\sum_{\ell=1}^{K_t^{g,i}} (\tilde{Z}_\ell^{g,i})^2 + \sum_{\ell \neq \jmath}\sum \tilde{Z}_\ell^{g,i} \tilde{Z}_\jmath^{g,i} | \tilde{K}_t^{g,i} = K_t^{g,i}\right)\right] && (3.12)\\
&= \cdots = \mathbb{E}(\tilde{K}_t^{g,i}) \cdot \sigma^2(\tilde{Z}^{g,i}) + \mathbb{E}[(\tilde{K}_t^{g,i})^2] \cdot \mathbb{E}(\tilde{Z}^{g,i})^2 && (3.13)
\end{aligned}$$

$$\sigma^2(\tilde{X}_t^{g,i}) = \mathbb{E}(\tilde{K}_t^{g,i}) \cdot \sigma^2(\tilde{Z}^{g,i}) + \sigma^2(\tilde{K}_t^{g,i}) \cdot E(\tilde{Z}^{g,i})^2 \tag{3.14}$$

With regard to the generating function of moments, with the hypotheses introduced and remembering its properties regarding the sum of independent variables and the properties regarding the univocity of the generating function of moments for a given probability distribution, one obtains:

$$\mathcal{M}_{\tilde{X}_t^{g,i}}(x|\tilde{K}_t^{g,i} = k) = \mathcal{M}_{\tilde{Z}_1^{g,i},\dots,\tilde{Z}_k^{g,i}}(x) \tag{3.15}$$

$$= \prod_{\ell=1}^{k} \mathcal{M}_{\tilde{Z}^{g,i}}(x) = \left(\mathcal{M}_{\tilde{Z}^{g,i}}\right)^{k} \tag{3.16}$$

$$\mathcal{M}_{\tilde{X}_t^{g,i}}(x) = \mathbb{E}\left(\mathcal{M}_{\tilde{X}_t^{g,i}}\left(x|\tilde{K}_t^{g,i} = k\right)\right) = \mathbb{E}\left[\left(\mathcal{M}_{\tilde{Z}^{g,i}}(x)\right)^{\tilde{K}_t^{g,i}}\right] = \tag{3.17}$$

$$=\mathbb{E}\left[e^{\tilde{K}_t^{g,i}\cdot\log\mathcal{M}_{\tilde{Z}^{g,i}}(x)}\right] = \mathbb{E}\left[e^{\tilde{K}_t^{g,i}\cdot\psi_{\tilde{Z}^{g,i}}(x)}\right] = \mathcal{M}_{\tilde{K}_t^{g,i}}\left(\psi_{\tilde{Z}^{g,i}}(x)\right) \tag{3.18}$$

Where $\psi_{\tilde{Z}^{g,i}}(x)$ is the generating function of cumulants[1] of $\tilde{Z}^{g,i}$. If the assumption of independence between severity and frequency of claims fails, it is possible to introduce a dependency between them using, for example, powerful mathematical tools such as copulas (e.g. Gunbel/Clayton copulæ).

3.2 Systemic Risks Modelling

Unlike the individual approach and the collective risk approach, the model analysed in this dissertation has a radically different point of view. This is because the other two models and, more generally, their derivatives, aim to study the aggregate cost of the claims of a pool of companies/policyholders by identifying common characteristics and reasoning in aggregate. They can be said to have a "macro" point of view. The model that will be explained below, however, reverses this viewpoint and adopts a "micro" one.

[1] The generating function of cumulants $\psi_{\tilde{X}}(x)$ is defined as the natural logarithm of the generating function of moments $\mathcal{M}_{\tilde{X}}(x)$: $\psi_{\tilde{X}}(x) = \log\mathcal{M}_{\tilde{X}}(x) = \log(\mathbb{E}(e^{x\cdot\tilde{X}}))$.

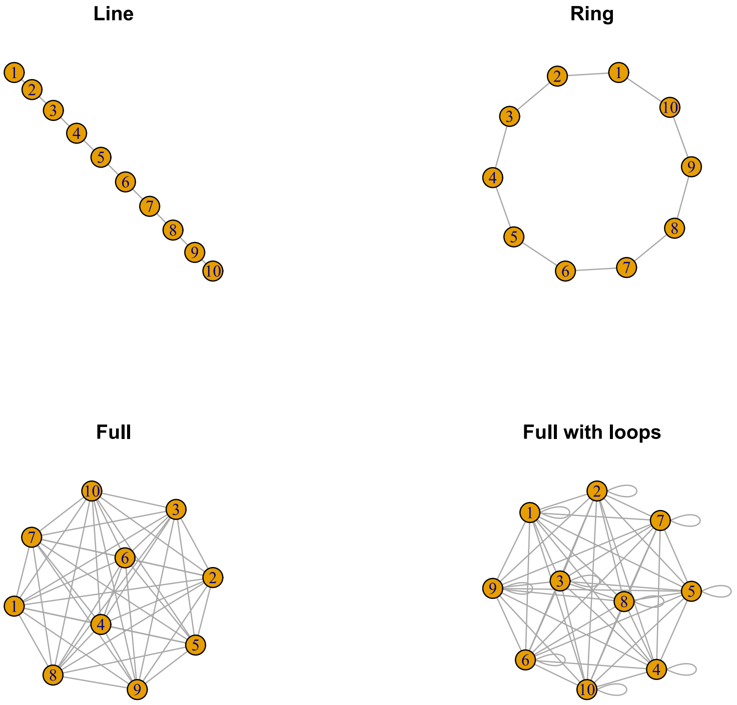


Figure 3.1: Generic networks

The core of the model is the characterisation of the individual company that decides to take out an insurance contract to protect itself against cyber risks. The contract, starting from certain characteristics deduced (or required) from the company, is then customised and adapted. As can easily be imagined, the calibration of the parameters of the selected distributions and the accuracy of the assumptions used come from historical data in the possession of the insurance company or are the result of expert judgement and in general may be more or less conservative.

The model attempts to reproduce the essential and minimal structure of communications within the company, schematising it using a graph (i.e. a Network) and attempting to reproduce communications within it. In this way, possible 'infections' due to a cyber attack and/or the dynamic spread of the same within the company can be simulated over the policy period.

Reproducing the internal and external communication structure of a company by means of networks means assuming that each node of a network can represent a PC, a device or even a server. The figure 3.1 shows some trivial examples of networks generated using the `igraph` package on `R`. Obviously, these are not realistic models of nodes and connections within a company, but they may be representative of the model. In all 4 graphs there are 10 nodes, for simplicity's sake we can assume that these are PCs. At a first qualitative glance, one can see that, depending on the topology of the network considered, there may be more or fewer connections, given the same number of nodes. A node may in fact communicate with no node, or with all the others, and in the last case, it may also communicate with itself. The latter is a case that will be discarded for convenience, because, thinking of an infectious dynamic, it makes no sense to assume that a node can be infected by itself.

From a practical point of view, the more connections possible, the greater the chance of infecting or being infected.

A broker or insurer is *unlikely* to be able to obtain the underlying topological structure of the company's communications. Some of these can be found in the literature, both from small and very large companies, mainly due to the leakage of the e-mail box. The effort on the part of the insured may be too great at the policy underwriting stage and may therefore discourage underwriting. The figure 3.2 shows the structure of a network of 167 employees of a manufacturing company[2]. It is internal email communication over a period of 9 months from 1 January 2010 to 30 September 2010. The data were made available in an anonymised manner and, in the case where there are several recipients of the same email (e.g. To, CC) they were represented in different rows in the data set provided.

As it can be seen from the picture, it is not at all easy to reconstruct the structure faithfully. In the literature, for example in [21], an attempt has been made to study the networks generated by e-mail communications within the company using different techniques such as Decision Trees, Random Forest, Neural Networks, Support Vector Machines and different clas-

[2] Source: `https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/6Z3CGX`

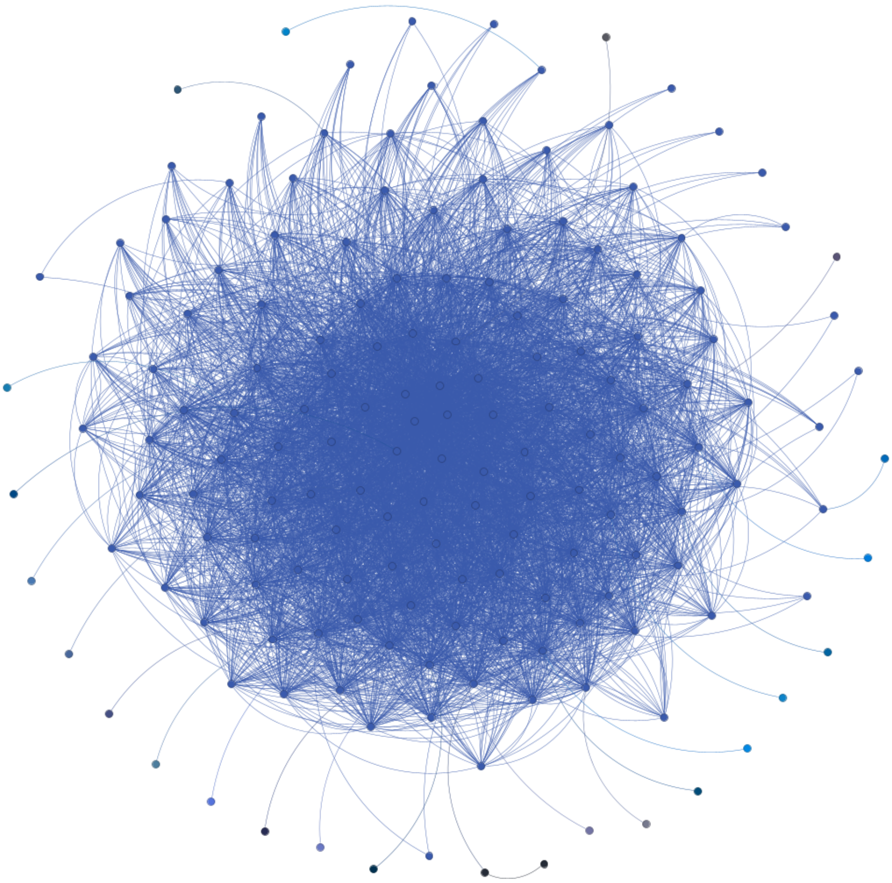


Figure 3.2: Manufacturing company e-mail communication

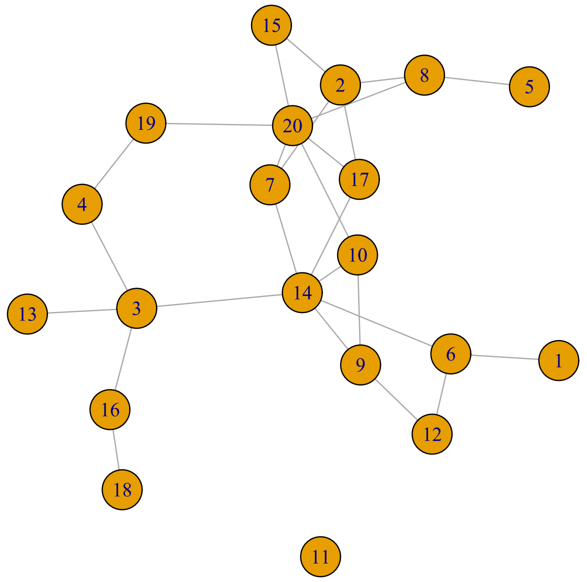


Figure 3.3: A simple graph

sification algorithms. It goes without saying that the internal dynamics of a large multinational company with different management models behave differently than a small medium-sized company or even a start-up with a handful of employees. What is not easy to reconstruct on a theoretical level is the hierarchy. It is therefore very difficult to rely solely on a database of emails, but it can be a good starting point if it is available to the insurer.

3.3 A gentle introduction on graph theory

The literature on graph theory is very extensive (see for example [23], [8] and [5]), given also the recent interest in recent years both in the field of social networks and in the field of epidemiology and the spread of epidemics, and consequently the study of relations between human beings and their connections. The first theorisations of graphs are very old now. A milestone in graph theory dates back to 1736, for example, where Euler tackled the "Königsberg bridge problem". The city (which is called Kaliningrad today) was and is traversed by a river and its tributaries. The problem consisted in demonstrating whether it was possible to cross all the bridges of the city in one walk and in such a way as to cross them once and only once. Euler came to the conclusion that it was not possible and was the first to state this by means of a mathematical proof.

In abstract terms, a *graph* can be defined as an *ordered tuple* consisting of a (finite) set $\mathcal{V}$ of vertices/nodes and a (finite) set of edges $\mathcal{E}$. In the figure 3.3, for example, we can see that node 19 is connected with node 20 and node 4. Consequently, it will be affected by two edges $(19-20, 19-4)$.

If two nodes are associated with the same edge then they are said to be two *end-vertices* of the edge e. Given a graph then two sets $\mathcal{V}(G) = \{v_1, v_2, \ldots, v_{n_\mathcal{V}}\}$ and $\mathcal{E}(G) = \{e_1, e_2, \ldots, e_{n_\mathcal{E}}\}$ can be derived and they constitute the sets of nodes and edges respectively. In the code chunk one can see the two sets for the graph of the figure 3.3.

```
> E(G)
+ 26/26 edges from b1b473b:
  3-- 4  1-- 6  2-- 7  2-- 8  5-- 8  9--10  6--12  9--12
  3--13  3--14  6--14  7--14  9--14 10--14  2--15  3--16
  2--17 14--17 16--18  4--19  7--20  8--20 10--20 15--20
  17--20 19--20

> V(G)
+ 20/20 vertices, from b1b473b:
 [1]  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20
```

Having defined the two sets $\mathcal{V}(G)$ and $\mathcal{E}(G)$ as finite, it is always possible to obtain the number of elements of these sets: $n_\mathcal{V} = |\mathcal{V}(G)|$, $n_\mathcal{E} = |\mathcal{E}(G)|$. In the graph in the example we have $n_\mathcal{V} = 20$ and $n_\mathcal{E} = 26$. This dissertation will deal with a particular subset of graphs called *simple graphs*. These are the graphs that contain no *loops* (i.e. cases in which a node is connected to itself) and no *multiple edges*. The latter case is when two nodes can be connected by two distinct edges. The graph in the figure 3.3 is therefore a simple graph and, unless explicitly stated, all graphs presented thereafter will be simple graphs.

Graphs can also be *directed* or *undirected*. A graph is directed if its edges have a direction. They can be thought of as arrows. Thinking of communication by email, it makes sense to assume that a generic link between two PCs, schematised except for one edge and two nodes, can be considered undirected, since communication is in most cases bidirectional. Another important characteristic of graphs attributable to both nodes and edges is the *weight*. This can be represented by a number. In the concrete case of business communication, the weight could symbolise the intensity of the connection between two nodes. The greater the weight, the greater the number of emails exchanged between the two nodes.

Another important characteristic referring to nodes is their *degree*. It is denoted by $\deg(n_1)$ and is simply the number of edges that the node possesses. In a graph, it is also possible to have nodes with degree zero, i.e. nodes that do not communicate with any other node. Furthermore, there is a relationship that links the degree of the nodes in a graph with the total number of edges $n_{\mathcal{E}}$:

$$2 \cdot n_{\mathcal{E}} = \sum_{v \in \mathcal{V}(G)} \deg(v), \quad n_{\mathcal{E}} = |\mathcal{E}(G)| \tag{3.19}$$

To be true, the relation needs to assume that the degree of a node with a loop is equal to 2.

Since the values that the degree can take are limited, the maximum and minimum degree of a node can be easily defined. In the following discussion, these definitions will be useful for investigating the existence of a relationship between the degree of a node and the probability of infection during insurance coverage. There is also a relationship that links the average degree with the number of vertices and nodes:

$$\Delta(G) = \max_{v \in \mathcal{V}(G)} \deg(v) \tag{3.20}$$

$$\delta(G) = \min_{v \in \mathcal{V}(G)} \deg(v) \tag{3.21}$$

$$\mathbb{E}\Big(\deg(G)\Big)_{v \in \mathcal{V}(G)} = \frac{2n_{\mathcal{E}}}{n_{\mathcal{V}}} \tag{3.22}$$

$$\delta(G) \leq \mathbb{E}\Big(\deg(G)\Big)_{v \in \mathcal{V}(G)} \leq \Delta(G) \tag{3.23}$$

Given that a complete graph with $n_{\mathcal{V}}$ vertices has exactly $\frac{n_{\mathcal{V}} \cdot (n_{\mathcal{V}}-1)}{2}$ edges, a *sparse* graph is defined as one such that:

$$n_{\mathcal{E}} << \frac{n_{\mathcal{V}} \cdot (n_{\mathcal{V}} - 1)}{2} \tag{3.24}$$

A similar definition can be given through the mean degree of the graph:

$$\mathbb{E}\Big(\deg(G)\Big)_{v \in \mathcal{V}(G)} = \frac{1}{n_{\mathcal{V}}} \sum_{v=1}^{n_{\mathcal{V}}} d_v << \frac{1}{n_{\mathcal{V}}} \cdot n_{\mathcal{V}} \cdot (n_{\mathcal{V}} - 1) = n_{\mathcal{V}} - 1 \tag{3.25}$$

where $n_{\mathcal{V}} - 1$ is the mean degree of a complete graph without loops.

Adjacency matrix A convention of 0 and 1 can be used to concisely indicate relationships within a graph. A relationship between two nodes is indicated with a 1 and a non-relation with a 0: $E \in \{0,1\}^{n_{\mathcal{V}} \times n_{\mathcal{V}}}$ In this case, it is possible to map all possible relationships within a graph by introducing an *adjacency matrix* **A**. It is a matrix of dimension $n_{\mathcal{V}} \times n_{\mathcal{V}}$ and has some interesting properties. The element A_{ij} is equal to 1 if there is a link between node i and node j and is equal to 0 if there is no link between the two former nodes. Considering a regular graph without loops, we have that the elements on the main diagonal will all be equal to 0. A feature that will be useful in the following of this dissertation is that an adjacency matrix of an undirected graph is always *symmetric*. An example of a trivial graph with its adjacency matrix can be seen in figure 3.4.

Interpreting the adjacency matrix is very straightforward. For example, the i-th row (i.e. the row of node i) contains, at the 1s, the list of column

$$\underset{n_{\mathcal{V}}\times n_{\mathcal{V}}}{A} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

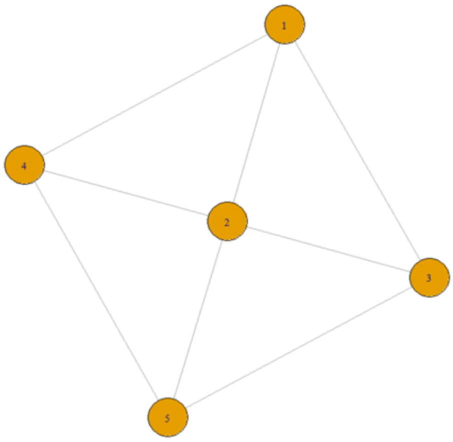


Figure 3.4: An example of an undirected graph with its adjacency matrix

indices (i.e. the other nodes) with which node i is connected. Thus, by summing up all the elements in the row, it is possible to obtain the degree of any node immediately.

$$\deg(v_i) = \sum_{j=1}^{n_{\mathcal{V}}} A_{ij} = \underset{1\times n_{\mathcal{V}}}{\mathbf{A}_i^T} \underset{n_{\mathcal{V}}\times 1}{\mathbf{1}} \tag{3.26}$$

Given a *symmetrical* matrix (such as the adjacency matrix of an undirected graph) we have that $\mathbf{A} = \mathbf{A}^T$ and that, if $\mathbf{A}\mathbf{x} = \lambda\mathbf{x}$ then for each $\mathbf{x} \in \mathbb{R}^n$ we have that $\mathbf{x}$ is an *eigenvector* and the corresponding λ is an *eigenvalue*. When a matrix is symmetric and contains real values (i.e. $\mathbf{A} \in \mathbb{R}^{n\times n}$, it is always the case that: *all* the eigenvalues of $\mathbf{A}$ are real, there exist eigenvalues $\lambda_1,\ldots,\lambda_n$ and eigenvectors $\mathbf{x}_1,\ldots,\mathbf{x_n}$ such that $\mathbf{x}_i^T\mathbf{x}_j = 0\ \forall i \neq j$ and the sum of the elements on the main diagonal of $\mathbf{A}$, i.e. the trace of A is equal to the sum of the eigenvalues:

$$\mathrm{trace}(\underset{n\times n}{\mathbf{A}}) = \sum_{\ell=1}^{n} a_{\ell\ell} = \sum_{\ell=1}^{n} \lambda_\ell$$

Given instead the *canonical basis* $\mathbf{e}_1,\ldots,\mathbf{e_n}$ where the element at the i-th position is equal to 1 and all other elements are equal to 0 (i.e. $e_i \in \{0,1\}$), one can define the *Laplacian matrix* of an undirected graph $G = (\mathcal{V},\mathcal{E})$ as:

$$\underset{n_\mathcal{V}\times n_\mathcal{V}}{\mathfrak{L}} = \sum_{(i,j)\in\mathcal{E}} (\mathbf{e}_i - \mathbf{e}_j)\cdot(\mathbf{e}_i - \mathbf{e}_j)^T \tag{3.27}$$

The Laplacian matrix can be obtained with the following relation:

$$\underset{n_\mathcal{V}\times n_\mathcal{V}}{\mathfrak{L}} = \underset{n_\mathcal{V}\times n_\mathcal{V}}{\mathbf{D}} - \underset{n_\mathcal{V}\times n_\mathcal{V}}{\mathbf{A}} \tag{3.28}$$

where $\mathbf{D} = \mathrm{diag}(d_1,\dots,d_{n_\mathcal{V}})$ is a diagonal matrix containing the degree of the nodes of the undirected graph. If the graph is weighted it is possible to define a matrix called *weighted Laplacian*:

$$\underset{n_\mathcal{V}\times n_\mathcal{V}}{\mathfrak{L}} = \sum_{(i,j)\in\mathcal{E}} w(i,j)\cdot(\mathbf{e}_i - \mathbf{e}_j)\cdot(\mathbf{e}_i - \mathbf{e}_j)^T \tag{3.29}$$

where $w(i,j) = 1 \iff (i,j) \in \mathcal{E}$ and $w(i,j) = 0 \iff (i,j) \notin \mathcal{E}$. Finally, given the matrix $\underset{n_\mathcal{V}\times n_\mathcal{V}}{W}$ the following equation holds:

$$\underset{n_\mathcal{V}\times n_\mathcal{V}}{\mathfrak{L}} = \underset{n_\mathcal{V}\times n_\mathcal{V}}{\mathbf{D}} - \underset{n_\mathcal{V}\times n_\mathcal{V}}{\mathbf{W}} \tag{3.30}$$

A final important relation concerning Laplacian matrices of undirected graphs is the following:

$$\underset{1\times n_\mathcal{V}}{\mathbf{x}^T}\underset{n_\mathcal{V}\times n_\mathcal{V}}{\mathfrak{L}}\underset{n_\mathcal{V}\times 1}{\mathbf{x}} = \sum_{(i,j)\in\mathcal{E}} (x_i - x_j)^2 \tag{3.31}$$

Proof.

$$\underset{1\times n_\mathcal{V}}{\mathbf{x}^T}\underset{n_\mathcal{V}\times n_\mathcal{V}}{\mathfrak{L}}\underset{n_\mathcal{V}\times 1}{\mathbf{x}} = \underset{1\times n_\mathcal{V}}{\mathbf{x}^T}\left(\sum_{(i,j)\in\mathcal{E}} (\underset{n_\mathcal{V}\times 1}{\mathbf{e}_i} - \underset{n_\mathcal{V}\times 1}{\mathbf{e}_j})(\underset{n_\mathcal{V}\times 1}{\mathbf{e}_i} - \underset{n_\mathcal{V}\times 1}{\mathbf{e}_j})^T\right)\underset{n_\mathcal{V}\times 1}{\mathbf{x}} = \tag{3.32}$$

$$= \sum_{(i,j)\in\mathcal{E}} \mathbf{x}^T(\mathbf{e}_\mathbf{i} - \mathbf{e}_\mathbf{j})(\mathbf{e}_i - \mathbf{e}_j)^T\mathbf{x} = \tag{3.33}$$

$$= \sum_{(i,j)\in\mathcal{E}} \Big(x(i) - x(j)\Big)\Big(x(i) - x(j)\Big) = \tag{3.34}$$

$$= \sum_{(i,j)\in\mathcal{E}} \Big(x(i) - x(j)\Big)^2 \geq 0 \tag{3.35}$$

and is valid $\forall \mathbf{x} \in \mathbb{R}^{n_\mathcal{V}}$.

Erdös Renyi Method It was mentioned earlier that obtaining granular data on a company's internal communications and of sufficiently high quality to trace back to a hierarchy and network is often too time-consuming for both agents of an insurance contract and hampered by privacy issues. Consequently, methods for creating networks with desired characteristics and properties are very useful. One of the main methods for generating networks of arbitrary size is called the Erdös-Renyi method.

This method makes it possible to generate an *undirected* graph with n nodes such that any edge occurs with a probability (chosen a-*priori*) p, independently of the other edges.

This implies that the degree distribution of a node of a graph generated by the Erdös-Renyi method follows the *binomial* distribution $\mathcal{B}(n_{\mathcal{V}}-1, p)$. It has the following probability density function:

$$\mathcal{P}\left(\tilde{\deg}(v) = d\right) = \binom{n_{\mathcal{V}}-1}{d} p^{d}(1-p)^{n_{\mathcal{V}}-1-d} \tag{3.36}$$

It implies that:

$$\mathbb{E}[\tilde{\deg}(v)] = (n_{\mathcal{V}}-1)p \tag{3.37}$$

$$Var(\tilde{\deg}(v)) = (n_{\mathcal{V}}-1)p(1-p) \tag{3.38}$$

When one wants to generate a network with a very large number of nodes, such that $n \to \infty$, then, by the *law of large numbers*, the degree distribution of a node follows a *normal distribution* $\mathcal{N}(n_{\mathcal{V}}p, n_{\mathcal{V}}p(1-p))$. When $n >> 0$ and a fixed lambda parameter equal to $n_{\mathcal{V}}p$ is set, then the binomial distribution tends to the *Poisson distribution* $Pois(\lambda = n_{\mathcal{V}}p)$.

There are other methods for randomly generating graphs. In fact, there exist methods for generating *scale-free* networks. The latter have a degree distribution of the graph nodes that follows a *power law* function, at least asymptotically. The famous *Barabasi-Albert* method, for example, exploits this type of scale-free network and combines the *preferential attachment* mechanism. In a nutshell, when generating the graph, the higher a node's degree, the more likely it is to receive new connections. This results in a dynamic that can be schematised in the phrase "*rich-gets-righer*".

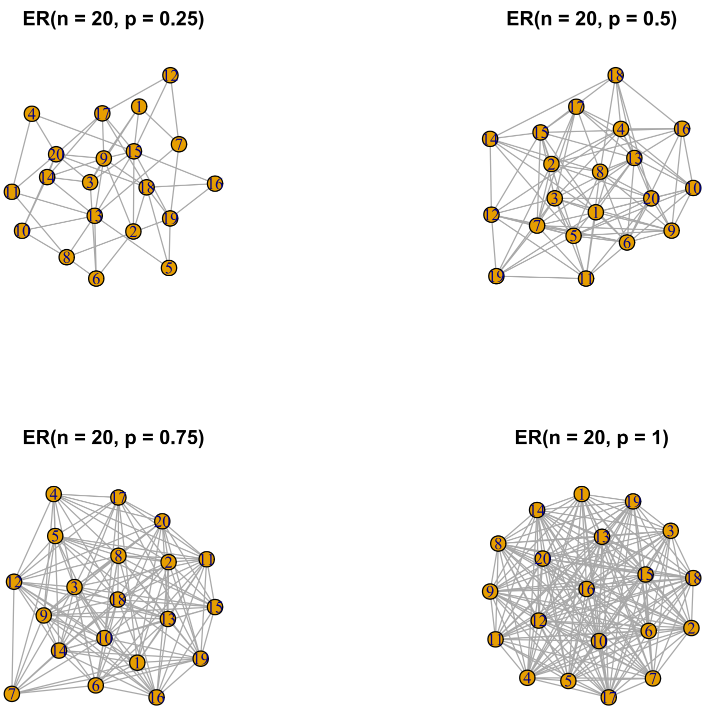


Figure 3.5: Erdös- Renyi example.

The figure 3.5 shows an example of the generation of 4 undirected networks using the Erdös-Renyi algorithm, holding the number of nodes $n_{\mathcal{V}}$ constant, but varying the probability p.

Once graphs have been created, it is possible to perform operations with them. First it is necessary to define what a *subgraph* is. A subgraph of a graph $G(\mathcal{V},\mathcal{E})$ is a graph $G'(\mathcal{V}',\mathcal{E}')$ such that $\mathcal{V}' \subseteq \mathcal{V}$ and $\mathcal{E}' \subseteq \mathcal{E}$. Obtaining subgraphs is very simple, it is sufficient to eliminate some nodes. Translating this mathematical concept to an example in reality, a subgraph of a graph representing a company communications network can be a department of the company or a small work group. The nodes of the department (and also their edges) will be included in the larger graph (the company) to which they belong.

It is also possible to obtain a subgraph, but by eliminating only cer-

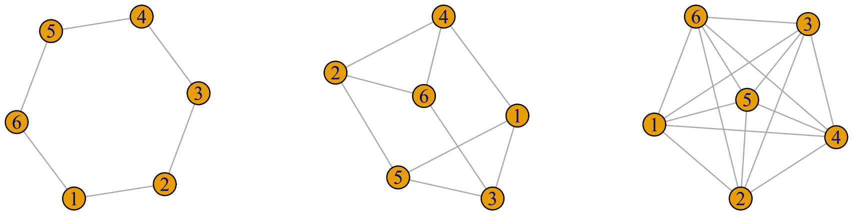


Figure 3.6: Example of a complementary of a graph (centre) and a union of the graph (left) and its complementary resulting in a complete graph (right).

tain connections (edges) while keeping the number of nodes within a network constant. This possibility may be common within a company, where, for example, communication between two departments cannot be allowed, keeping them strictly separated. Other natural operations for graphs are the *union* of two graphs and the *intersection* between graphs. A union occurs when taken $G_1(\mathcal{V}_1,\mathcal{E}_1)$ and $G_2(\mathcal{V}_2,\mathcal{E}_2)$, the union $G_1 \cup G_2$ is a graph $G_3(\mathcal{V}_2,\mathcal{E}_3)$ such that the set of nodes $\mathcal{V}_3 = \mathcal{V}_1 \cup \mathcal{V}_2$ and the set of edges is $\mathcal{E}_3 = \mathcal{E}_1 \cup \mathcal{E}_2$. Conversely, the intersection of $G_1 \cap G_2$ gives another graph $G_4(\mathcal{V}_4,\mathcal{E}_4)$ such that $\mathcal{V}_4 = \mathcal{V}_1 \cap \mathcal{V}_2$ and $\mathcal{E}_4 = \mathcal{E}_1 \cap \mathcal{E}_2$.

A further example of an operation possible with graphs is the *complement* of a graph. This graph is obtained by considering the same starting nodes as the original graph, but the set of edges must be the complementary $\bar{\mathcal{E}}$ of the set of starting edges $\mathcal{E}$. An example of this operation can be seen in figure 3.6.

But what is the relationship between a graph and the spread of communication within it? Definitions such as *walk* and *path* come to the rescue. A walk of length ℓ is a subgraph of the source graph that contains exactly ℓ edges. It differs from the path which has no repeated nodes and consequently has all different edges. With these definitions it follows that two nodes can be said to be connected if there is some walk of finite length that allows the second node to be reached from the first and vice versa. To know how many walks of length ℓ are possible from node i to node j, it is necessary to raise the adjacency matrix associated with the graph to the ℓ-th power. For example:

$$\underset{4\times4}{\mathbf{A}} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad \underset{4\times4}{\mathbf{A}} \cdot \underset{4\times4}{\mathbf{A}} \cdot \underset{4\times4}{\mathbf{A}} = [\underset{4\times4}{\mathbf{A}}]^3 = \begin{bmatrix} 0 & 4 & 4 & 0 \\ 4 & 0 & 0 & 4 \\ 4 & 0 & 0 & 4 \\ 0 & 4 & 4 & 0 \end{bmatrix} \tag{3.39}$$

3.4 Function `make_a_matrix`

The previous section introduced two main methods (Erdos-Renyi and Barabasi-Albert) for the random generation of networks with certain desired characteristics. In this section, a proposal for a function to generate a graph having certain characteristics chosen *a-priori* will be presented. The function appears as follows:

```
    G = make_a_matrix(num_groups,
                  size_group,
                  p_within,
                  p_between,
                  num_criticals,
                  p_criticals,
                  overlapping,
                  intensity_overlapping,
                    overlapping_quota)
```

The first parameters of the function are `num_groups` and `size_groups`, which together with the parameters `p_within` and `p_between` form the core of the function. Suppose, for example, that one wants to create a network that reproduces communication between 5 groups of approximately 20 people each. In this case `num_groups` would be equal to 5 and `size_groups` to 20. The next two parameters can be chosen at will, but the underlying assumption is that communication within groups is more frequent than communication between groups. To replicate this concept in the algorithm by which the function shapes the matrix, it is sufficient to choose a parameter `p_within` greater than `p_between`. These two parameters, being probabilities, must necessarily be between 0 and 1. In the Equation 3.40, one can see how the algorithm proceeds. While it is true that the parameters are fixed, it is equally true that the subgraphs that are aggregated are randomly generated and thus the groups will all be different from each other, by construction. First, the algorithm creates a matrix of adjacency matrices of Erdös-Renyi graphs ($n =$ `size_groups`$, p =$ `p_within`), `size_groups` by `size_groups` on the main diagonal. All other matrices of the largest starting matrix will be set equal to *zero*.

$$\underset{(ng+sg)\times(ng+sg)}{\mathbf{M}^{(I)}} = \begin{bmatrix} \underset{sg\times sg}{\mathbf{ER}} & \underset{sg\times sg}{\mathbf{0}} & \cdots & \underset{sg\times sg}{\mathbf{0}} \\ \underset{sg\times sg}{\mathbf{0}} & \underset{sg\times sg}{\mathbf{ER}} & \cdots & \underset{sg\times sg}{\mathbf{0}} \\ \vdots & \vdots & \ddots & \vdots \\ \underset{sg\times sg}{\mathbf{0}} & \cdots & \underset{sg\times sg}{\mathbf{0}} & \underset{sg\times sg}{\mathbf{ER}} \end{bmatrix} \tag{3.40}$$

The next step can be seen in the Equation 3.41. The matrices of zeros are replaced with matrices in which the elements are extracted from a Bernoulli with parameter `p_between`.

$$\underset{(ng+sg)\times(ng+sg)}{\mathbf{M}^{(II)}} = \begin{bmatrix} \underset{sg\times sg}{\mathbf{ER}} & \underset{sg\times sg}{\mathbf{A}_{12}} & \cdots & \underset{sg\times sg}{\mathbf{A}_{1,ng}} \\ \underset{sg\times sg}{\mathbf{A}^{T}_{12}} & \underset{sg\times sg}{\mathbf{ER}} & \cdots & \underset{sg\times sg}{\mathbf{A}^{T}_{2,ng}} \\ \vdots & \vdots & \ddots & \vdots \\ \underset{sg\times sg}{\mathbf{A}^{T}_{1,ng}} & \cdots & \underset{sg\times sg}{\mathbf{A}^{T}_{2,ng}} & \underset{sg\times sg}{\mathbf{ER}} \end{bmatrix} \tag{3.41}$$

Since the adjacency matrices of undirected graphs must be symmetrical, it will only be necessary to generate the matrices above the main diagonal and transpose them to the correct position at the bottom of the largest adjacency matrix. In this way one is sure, by construction, that symmetry is maintained.

In the Table 3.1, the parameters of two examples can be read, and the results (suitably transformed from adjacency matrices to igraph objects) can be viewed in Figure 3.7.

Table 3.1: Examples of 2 random graphs generated using `make_a_graph` function.

Parameter	*Example A*	*Example B*
`size_group`	20	10
`num_groups`	3	5
`p_within`	0.8	0.9
`p_bewteen`	0.1	0.2

Critical nodes Until now, undirected graphs formed by groups of fixed numerosity and connected with with any intensity within groups and between distinct groups have been created. The `make_a_matrix` function also allows intruding nodes, called *criticals* that symbolise particularly delicate structures of a company. This may be the case for particularly delicate servers, databases, or PCs, whose damage could be *far greater* than for a "normal" node. To add any number of critical nodes, simply start from the Equation 3.41 and expand it. By assumption of the model the critical nodes are *never connected* to each other, but rather are connected with a probability `p_criticals` with the other groups. In continuity with the previous

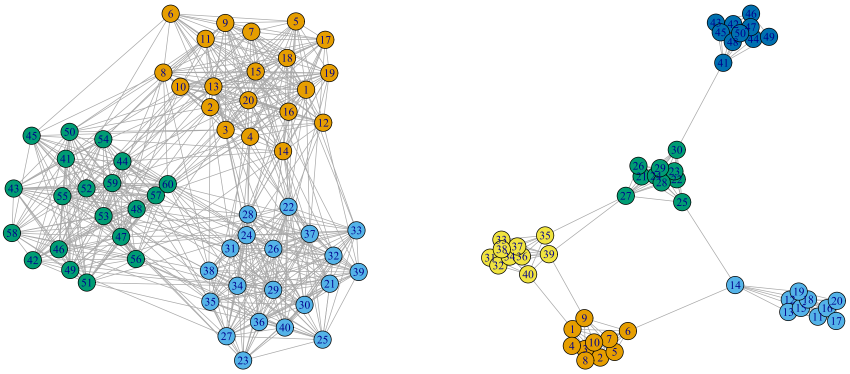


Figure 3.7: Example A and Example B

steps, this $\mathbf{M}^{(III)}$ matrix must also be symmetric at the end of the step.

$$\underset{(ng+sg+nc)\times(ng+sg+nc)}{\mathbf{M}^{(III)}} = \left[\begin{array}{c|ccc} \underset{(ng+sg)\times(ng+sg)}{\mathbf{M}^{(II)}} & & \underset{(ng+sg)\times nc}{\mathbf{C}} & \\ & 0 & \cdots & 0 \\ \underset{(ng+sg)\times nc}{\mathbf{C}^{\mathrm{T}}} & \vdots & \ddots & \vdots \\ & 0 & \cdots & 0 \end{array}\right] \tag{3.42}$$

Further mathematical details of the step can be seen in the Equation 3.42. An example of a graph with 60 nodes divided into 3 groups and 2 critical infrastructures can be seen in Figure 3.8. The `make_a_matrix` function allows (with a lot of flexibility) to choose how intense the communications of the critical nodes should be with the rest of the network. As will be seen in the rest of the dissertation, since the damage of the critical nodes assumed to be much greater than a normal node, the greater the intensity of the links, the greater the overall damage to the network could be.

Overlapping So far, graphs have been created given a number of groups and with desired properties such as the intensity of communication within the same group and between distinct groups. Another feature of the `make_a_matrix` function that gives it additional flexibility is the possibility of overlapping

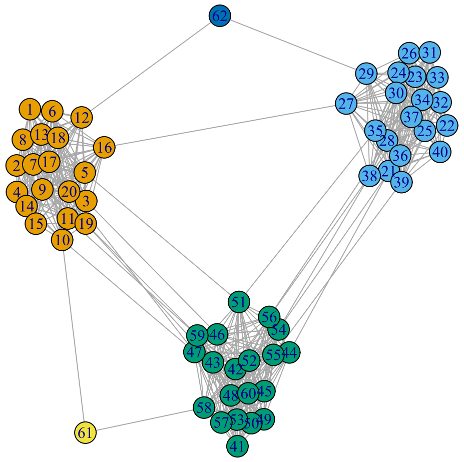


Figure 3.8: Graph with 2 critical nodes/infrastructures

between groups. In fact, one could have a situation in which two groups of employees formally belong to different departments, but have such dense and recurring communications that, at first glance, they cannot be distinguished from one another or from other groups. This can be a very common case and it is therefore good that the function provides for this feature. The overlapping parameter is simply a variable of type *logical*. If it is equal to `TRUE`, the other two parameters, which are `overlapping_quota` and `intensity_overlapping`, are read. The first allows to choose the percentage of groups in the graph that have overlapped with other groups. Specifically, the function takes all possible combinations of two from the vector of groups. For example, given 4 groups:

```
> vector_groups <- 1:4
> combinations <- t(combn(vector_groups,2))
> combinations
     [,1] [,2]
[1,]    1    2
[2,]    1    3
```

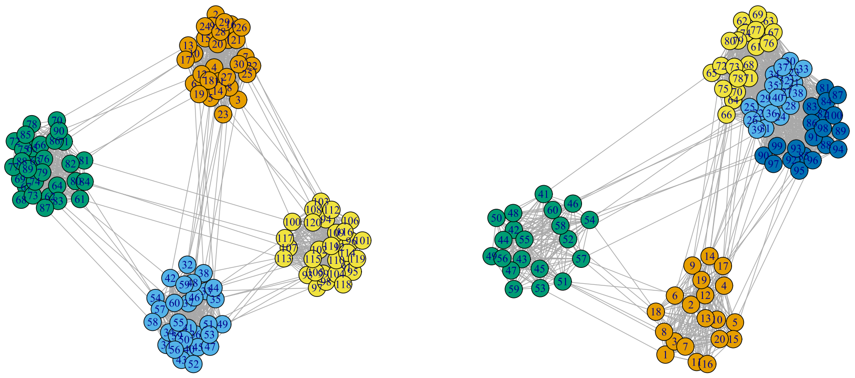


Figure 3.9: Examples of 4-group graphs without overlapping and with overlapping

```
[3,]    1    4
[4,]    2    3
[5,]    2    4
[6,]    3    4
```

Once all combinations are available, the function extracts the pairs without repetition and, at the adjacency submatrices of those pairs (i.e. $\underset{np\times np}{\mathbf{A}_{ij}}$), regenerates the Erdös-Renyi adjacency matrices, this time increasing the probability p.This does not change either the groups they belong to or the number of initial nodes, it simply increases the number of connections between those two extracted groups. An example of a graph with overlapping can be seen in Figure 3.9. The two graphs shown have been generated with the same parameters, simply the one on the left has no overlapping, while the one on the right does.

3.5 From an unweighted graph to a weighted graph

As pointed out in [31], it is also very important to use a *graph mining approach* (GMA) when dealing with graphs and more generally with communications within a network. The techniques used by GMA make it possible to identify patterns and characteristics intrinsic to a graph and thus to analyse it in greater detail. Essential the graph mining approach is the study of weights. As illustrated above, the weight is simply a number that is usually assigned to each edge, but can also be assigned to a node. Referring to a business communication graph, the weight is a measure of the intensity of communication between two nodes. During the duration of an insurance contract (e.g. 1 year) an edge between node i and node j only means that there has been at least one communication between the two nodes during the observation period. Probably if one does not often receive emails from an address, one is less likely to click on malicious links or give out personal information. Conversely, if one exchanges many e-mails with another node, one is more likely to let one's guard down.

Being able to calculate the communication intensity and thus a weight for each edge also makes it possible to simplify a model for the spread of viruses and malicious attacks in a corporate network. Depending on certain thresholds and a predetermined risk level chosen by the company, it is possible to implement connection filtering, removing those sporadic connections that are not sufficiently harmful in a spreading dynamic. This activity is very crucial, especially when dealing with a large number of nodes, and from a computational point of view, as will be shown later on, these are aspects to be taken into account.

In this dissertation, as was explained earlier, the focus is on trying to recreate a network that is true to real dynamics, through a flexible model that is mostly focused on small to medium-sized enterprises. For this reason, it is necessary to identify a method for assigning weights to the generated edges. There are two macro-approaches in the literature: node-based method and edge-based method. In this dissertation, a variation of the second method described in [31] was used. The basic concept is relatively simple, for each day of the contract duration, the number of communications that have taken place are generated according to a certain discrete distribution and, with a certain criterion, these communications are distributed to the edges. Consequently, during the contract period, some edges may have a very low weight e.g. $2, 3$ or even a very high weight such as $2,000$

i.e. about 5 emails per day between the same two nodes.

A proposal for an algorithm to assign weights Suppose that the input is a total number of internal conversations that occur every day. Assume to take as the *mean* of the distribution a number equal to:

$$\mathbb{E}(\tilde{X}) = n * \text{number of nodes}$$

In this dissertation, this number was used as the mean of a *Negative Binomial*. This distribution was used because, given the fact that it is a *mixture* of the discrete *Poisson distribution* in the particular case where the structure variable of the Poisson is a *Gamma distribution* with equal parameters, it has *greater* variability.

In R, the Negative Binomial distribution requires two input variables:

- `size` which is equivalent to the shape parameter in the case of the mixture of the Gamma distribution;

- `prob` which is the probability of success in each trial.

$$\tilde{X} \sim Po(n \cdot \tilde{q}), \quad \tilde{q} \sim Gamma(h,h), \quad \mathbb{E}(\tilde{q}) = \frac{h}{h} = 1 \tag{3.43}$$

$$\tilde{X} \sim NB(h,p), \quad p = \frac{h}{h+n} \tag{3.44}$$

$$\mathbb{E}(\tilde{X}) = n = \frac{1-p}{p} \cdot h \tag{3.45}$$

$$\text{if } n = 20 \cdot \text{num\_nodes} \Rightarrow h = n \cdot \frac{p}{1-p} \tag{3.46}$$

Once the two main parameters of the Negative Binomial distribution have been identified (using the equations written above), it is possible to use them to generate the number of communications occurring each day in the network and *redistribute* them in the edge list of the starting graph. To extract the edges of the nodes where communications occur, one can use the `sample` function of R. To add even more variability and avoid, using the default parameters of the function, that on average all edges have the same number of communications per day, one can specify a *custom* vector

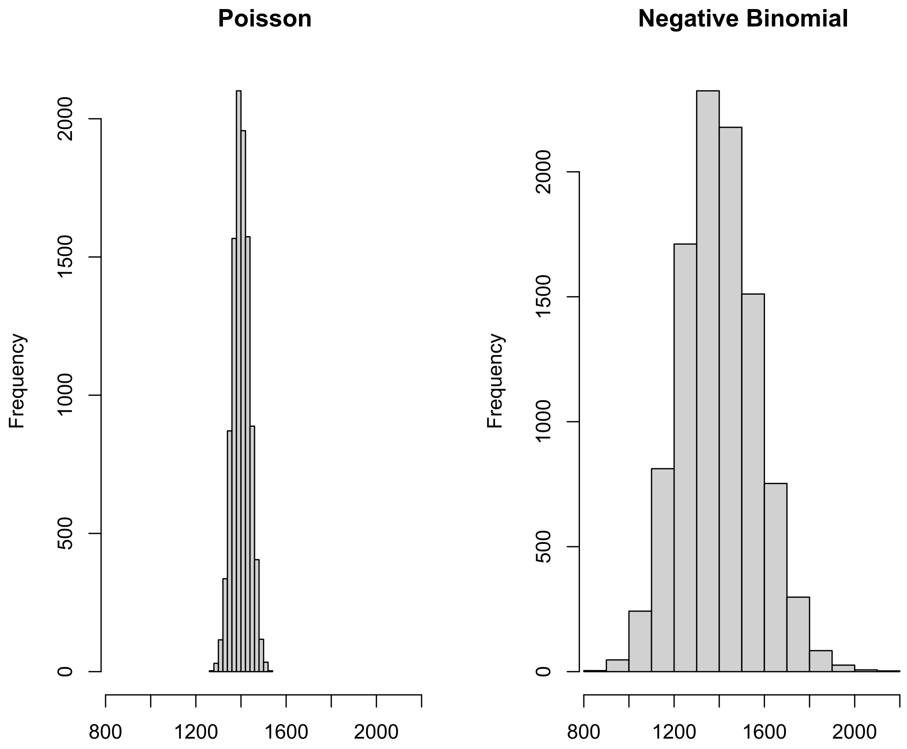


Figure 3.10: Histograms of total number of daily communications.

of probabilities. The vector can be calculated using either a *Uniform distribution* or a *Beta distribution*. Following this approach, each day, one will have edges that have had many more communications than others, for the same total daily communications.

In the Figure 3.10 one can see two examples of histograms obtained by simulating the total number of communications occurring in a day using either a Poisson distribution or a Negative Binomial distribution. As can be seen, the histogram in the case of the Poisson is very *concentrated* around the mean, whereas the second allows for greater variability in the results. It is easy to imagine that during the year there may be periods of more intense communications. However, the model is flexible and, if desired, a uniform distribution can be assumed.

With this approach, however, given a high number of communications

Table 3.2: Example of daily weights for the 10 edges.

Edge	*Frequency*	*Edge*	*Frequency*
1	4	13	1
3	3	14	1
7	5	16	1
9	7	17	2
12	2	19	2

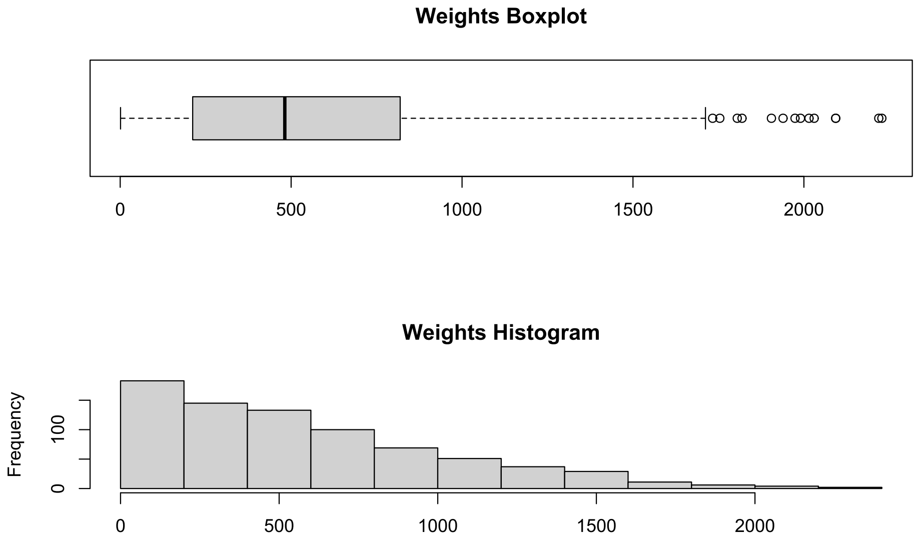


Figure 3.11: Example of boxplot and histogram of annual weights.

and given a not so high number of edges, the probability of each edge being affected by at least one daily communication would be too high. In reality, many communications between certain edges occur only a couple of times a year and are often unidirectional. To overcome this problem, when simulating the number of communications on an i-day, one can extract with a binomial which edges will be affected by a communication (1) and which will not (0). In this case, as the chosen parameters of the Binomial Distribution change, it will be possible to distribute the total number of communications among a greater or lesser number of edges.

Table 3.2 shows an example of an extraction for 10 edges on an *i*-th day. As can be seen, edge 1 was affected by 4 communications, edge 12 by 2 communications and so on. In Figure 3.11 one can see the histogram of the weights for a network of about 70 nodes, assuming an average of $20 * (number\ of\ nodes)$ communications per day. A strong *positive* asymmetry can be seen from the histogram, from which it can be deduced that only a small subset of edges have a high weight, while most have a lower weight. What is important is that, given the structure of the graph, it is possible in the context of policy pricing to personalise the assignment of weights and make it customer-specific. To simplify the structure of the network as well, one can also imagine eliminating all those edges that have a weight below a certain threshold and thus classify them as non-significant.

3.6 Epidemiological models for cybersecurity insurance

Up to this point, a method was described for generating random graphs that have certain characteristics as much in common as possible with a business communication network. The weights are then assigned to the edges according to a certain criterion. In this section, methods for reflecting and simulating an infectious dynamic within a company will be discussed. The purpose is quickly stated: an attempt is made to simulate infection between the company's nodes (criticals and non-criticals) and to simulate the possible damage due to these attacks during the policy coverage period. The insurer or underwriter will then be able to identify, thanks to the simulations, a premium to cover the expected losses.

The first works in the literature concerning the study and modelling of infections and their dynamics in a population are now almost a century old. See for example the [15] pioneering work of 1927.

The epidemiological models used to study computer-related infections, however, are quite recent. They started to spread with the malicious spread of viruses such as worms. See, for instance, the article of [19], which analysed years of infection data on the *'Conficker'* worm, which exploited and still exploits windows vulnerabilities to transmit itself from device to de-

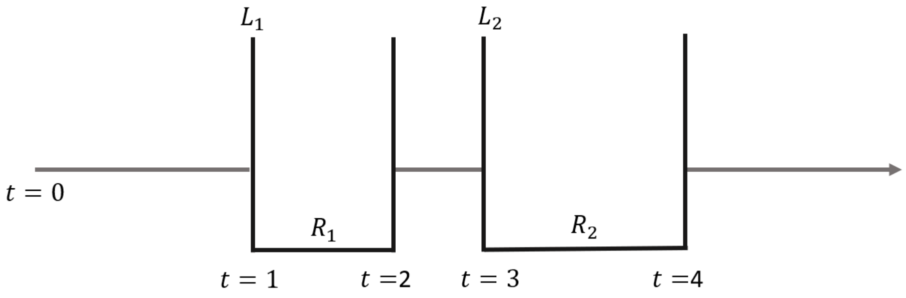


Figure 3.12: Infection-recovery scheme for a node ℓ

vice, also thanks to external media such as USB pen-drives. The work, on the other hand, that has been directed not only at the study of infections in a corporate system, but also at the pricing of insurance products is more recent and is still considered pioneering work. See, for example, the articles by [16], [30], [12] and [26].

In this dissertation, an epidemiological model will be presented that takes inspiration from the [30] and [31] models by implementing appropriate modifications.

In order to translate the dynamics of infection within a network into mathematical concepts, it is necessary to introduce a variable relating to each node and each time instant considered: the status of a node. Given an undirected and weighted graph at a certain time instant t a node in the graph is defined as *secure* if it is not currently under attack, but is *vulnerable/susceptible* to an attack. Conversely, a node is said to be *infected* if it has been the victim of an attack (or is still under attack) and one must wait for the necessary time to restore its functionality. The time variable can instead be considered *discretely* or *continuously*. In this dissertation, it will be considered as a continuous variable. At each time instant t, it is therefore necessary to know the status of each node and, by extension, the status of the network.

The status of a graph $G(\mathcal{V},\mathcal{E})$ can be represented in mathematical terms by a vector of realisations of random variables of length $n_{\mathcal{V}}$:

$$\Big(I_1(t), I_2(t), \ldots, I_{n_{\mathcal{V}}}(t)\Big) \tag{3.47}$$

such that

$$\tilde{I}_\ell(t) = \begin{cases} I_\ell(t) = 1, & \text{infected} \\ I_\ell(t) = 0, & \text{secure} \end{cases} \tag{3.48}$$

It represents the status of the ℓ-th node. It is equal to 1 when the node is infected and is equal to 0 when the node is secure but susceptible to infection.

For this reason, it is important to know for each node and for each time instant the *probability vector*:

$$\Big(p_1(t), p_2(t), \ldots, p_{n_{\mathcal{V}}}(t)\Big) \tag{3.49}$$

such that

$$p_\ell(t) = \mathcal{P}(I_\ell(t) = 1) \tag{3.50}$$

An attack may come from a threat within the network itself or from outside. For instance, consider the case where a malicious link is opened from an address outside the organisation. In this case, the attacker could take control of the company's internal email list and also the account of the victim. The threat from this point would then be an inside threat. Figure 3.12 shows how an attack and recovery of a generic node is modelled. At instant $t = 0$, node ℓ is secure, but susceptible to an attack. At a certain instant $t = 1$, the node is the victim of an attack and instantaneously suffers L_1 damage. From then on until $t = 2$ the node is considered not susceptible to further attacks and needs time (also random) for repairs. Repair also has a cost (R_1). At $t = 2$ the node becomes secure again, but susceptible and at $t = 3$ it suffers a second attack and further damage L_2[3]. Then time elapses for the recovery process (and another recover cost R_3) and the node returns secure etc.

[3] It should be noted that the notation $t = 2$ and $t = 3$, for example, does not mean that only one instant of time has elapsed e.g. 1 day, but can be a fraction of a day as well as tens of days.

This type of infection dynamics in epidemiology is called the SIS model. In the field of cyber infections, it has been studied in depth by [26] and [29]. More generally, the $\varepsilon - SIS$ model is a variation of the SIS epidemiological model. They are three so-called *compartmental models* because precise assumptions are made to simplify the dynamics of infection (usually of infectious diseases, but the same reasoning extends to computer viruses and hacker attacks) and they are called compartmental models because the population is divided into a few distinct categories. Within them, however, the characteristics are the same.

In the case of the SIR model, the compartments considered are Susceptible, Infectious and Recovered. In this case, once a node is recovered it gains an immunity that may be more or less long. Extending this to an insurance contract, if an SIR model were used, a PC once infected could no longer be infected again during the contract term. However, this situation is unrealistic. For this reason, it is more advisable to use a SIS model, i.e. Susceptible, Infectious and Susceptible. In the epidemiological/medical field, this situation exists with viruses such as influenza or the common cold, which often give such a short-lived immunity that it can almost be disregarded. In cyber insurance, an SIS model allows a node, once cured, to be immediately reinfected. The parameters used in the SIS model are β and δ. β is the parameter describing the dynamics of infection, while δ is the parameter describing the dynamics of recovery. In classical modelling, the infection/recovery process is seen as a *renewal reward process*.

The renewal reward process is a generalisation of the Poisson process. The difference between the two is that although the holding times must be *i.i.d.* (independent and identically distributed), with *finite mean* and with *positive support*, the renewal reward process admits distributions other than the exponential. Consequently, when exponential distributions are used, one is dealing with a *Markov Model* (M), vice versa with a *Non-Markov Model* (N).

Markov Model In this case (M) the infection process per link is a *Poisson process* with *rate* β and the recovery process is a *Poisson process* with rate δ. An extension of the SIS model is the $\varepsilon - SIS$ model. ε then becomes the rate parameter of a *Poisson process* that simulates the (self) infection of the outside of the network. Each node can therefore at any instant in time, if secured, be infected either by infected *neighbours* (i.e. other nodes with which it communicates) or by a threat outside the network, and this is where the epsilon parameter comes into play.

In formulæ:

$$\begin{cases} I_\ell(t): 0 \to 1 \text{ at rate } \beta \sum_{i=1}^{n} a_{\ell i} I_i(t) + \varepsilon_\ell \\ I_\ell(t): 1 \to 0 \text{ at rate } \delta_\ell \end{cases} \tag{3.51}$$

Thus it follows that the status for node ℓ at time t goes from 0 to 1 considering a rate that is a function of the parameter β (constant for all nodes), the adjacency matrix (the ℓ-th row) and the status of the neighbouring nodes as well ($I_i(t)$) as the self infection rate ε. The latter may vary as the node considered varies or be held constant. The transition of status from 1 to 0 (i.e. the recovery of the node) is solely a function of the rate δ_ℓ which may vary as the node varies or be held constant for all nodes. Such a Markov Model, however, does not allow for much customisation. The nodes are essentially all considered the same and the weights of the edges are not taken into account in any way. This means that there is no difference if one node communicates with another that is infected but has a weight of 1 or 2000. This is implausible in reality since a phishing or social engineering attempt is much more likely to succeed if one is contacted by people with whom one is more likely to let one's guard down and with whom one feels safer. It is unlikely that one will give up his/her credentials to a contact in the company that he/she hears from very occasionally. The advantages of this model, however, are its simplicity and interpretability. The parameters to be calibrated are few and can be easily explained to those who have no particular expertise in networks and/or epidemiological models.

In the Figure 3.13, the two SIS and $\varepsilon - SIS$ schemes can be seen in comparison. From the $\varepsilon{-}SIS$ model, one can truly understand why a line of business such as cybersecurity insurance can be a difficult LoB to price. The ε rate means that the graph is under constant threat from the outside and it

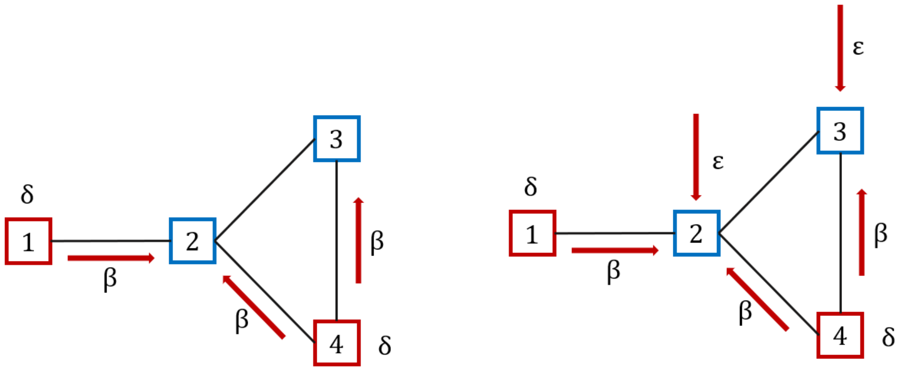


Figure 3.13: SIS and $\varepsilon - SIS$ models

is therefore not enough just to monitor internal company communications.

Non-Markov Model This model is more general and therefore more customisable and has been adopted in this dissertation. In a nutshell, in a Non-Markov model the time to infection for any node at any time instant is given by the minimum of the times to infection generated by random variables $\tilde{Y}_1, \ldots, \tilde{Y}_{D_\ell}$ (where D_ℓ are the infected neighbours of the node ℓ) and $\tilde{Z}_\ell$ which is the self infection time (for threats from outside the network):

$$\tilde{T}_\ell = \min\left(\tilde{Y}_1, \ldots, \tilde{Y}_{D_\ell}, \tilde{Z}_\ell\right) \tag{3.52}$$

The recovery time for an infected node is Rv. It is important to note that even in the non-markov model, once a node has been infected, it cannot suffer further attacks until it is restored.

A proposal From the previous Markov models [31] described two further generalisations: the $H{-}SIS$ and $HG{-}SIS$ models. The scheme of these two models is depicted in Figure 3.14.

The first is a heterogeneous SIS model. Basically, it is the same as the SIS model, but the beta rates are different for each link. The underlying rationale is that the rate should be larger the greater the intensity (weight) of the link between two nodes. This is because it is assumed that the probability of infection increases if the two nodes communicate a lot with each

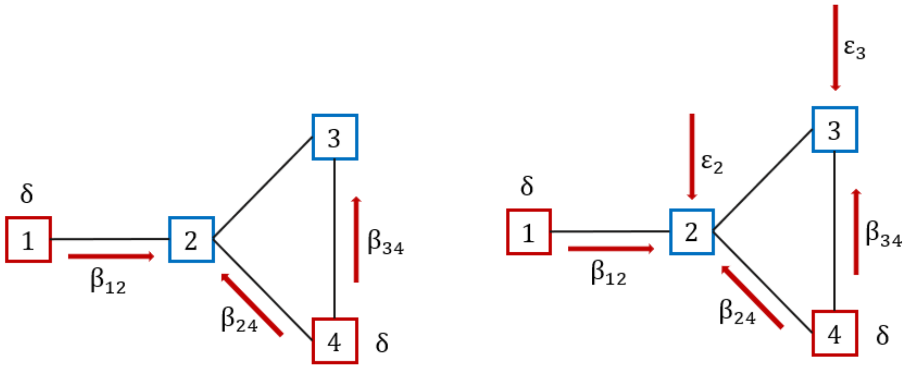


Figure 3.14: $H-SIS$ and $HG-SIS$ model.

other and thus the times to infection are reduced. The second model is the $HG-SIS$ and is basically an $H-SIS$ model, but with self infection probability. So the betas change depending on the link considered and each node has a self infection probability. The betas in all 4 epidemiological models considered remain constant.

The *downsides* of these last two models are that instead of having to estimate and 3 parameters, it is necessary to estimate as many betas as there are edges in a graph. This is potentially a large number of estimates to be made. This is why [31] has proposed a method to greatly simplify this procedure. Basically, one chooses a minimum and maximum beta value and by means of a *sigmoidal transformation* one obtains a matrix of betas. It is a matrix because one has a beta for every 1 in the adjacency matrix of the graph considered. Since by hypothesis it is considered an undirected graph, the betas above the main diagonal of the matrix remain to be estimated. It goes without saying that at the 0s of the adjacency matrix there is also a weight of zero, while the minimum weight value of an edge is 1.

The proposed transformation is a function of the weight of the edge considered, the minimum and maximum beta and the value of k:

$$f(w_{ij}) = \begin{cases} 0, & w_{ij} = 0 \\ \frac{\beta-\delta_\beta}{1+exp(-k(w_{ij}-\bar{w}))} + \delta_\beta, & w_{ij} > 0 \end{cases} \tag{3.53}$$

$$\bar{w} = \frac{1}{2 \cdot |\mathcal{E}|} \sum_{i,j} w_{ij} \tag{3.54}$$

$$k = \frac{1}{\sigma} \tag{3.55}$$

$$\sigma = \frac{\sum_{i,j} |w_{ij} - \bar{w}|}{2 \cdot |\mathcal{E}|} \tag{3.56}$$

$$\underset{n_{\mathcal{V}} \times n_{\mathcal{V}}}{\mathbf{B}} = \begin{bmatrix} 0 & \frac{\beta - \delta_\beta}{1+exp(-k(w_{12}-\bar{w}))} + \delta_\beta & \cdots & \frac{\beta - \delta_\beta}{1+exp(-k(w_{1n_{\mathcal{V}}}-\bar{w}))} + \delta_\beta \\ \frac{\beta - \delta_\beta}{1+exp(-k(w_{21}-\bar{w}))} + \delta_\beta & 0 & \cdots & \frac{\beta - \delta_\beta}{1+exp(-k(w_{2n_{\mathcal{V}}}-\bar{w}))} + \delta_\beta \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\beta - \delta_\beta}{1+exp(-k(w_{n_{\mathcal{V}}1}-\bar{w}))} + \delta_\beta & \frac{\beta - \delta_\beta}{1+exp(-k(w_{n_{\mathcal{V}}2}-\bar{w}))} + \delta_\beta & \cdots & 0 \end{bmatrix} \tag{3.57}$$

The new beta values may differ depending on the edge and the desired interaction. It is indeed possible (and will be used in the simulations) to consider different (minimum and maximum) beta values depending on the node type. If, for example, a critical node is considered, one can consider smaller minimum and maximum betas in absolute value than those used for "normal" nodes. Then, always applying the sigmoidal transformation according to weight, it will be possible to obtain minimum and maximum beta values and smaller average times to infection.

Thanks to this particular type of transformation, one can obtain properties relating to betas that are of interest. Four of these are identified in [31] and are mostly asymptotic results:

- $\max(\beta_{ij}) = \beta \land \min(\beta_{ij}) = \delta_\beta$: this is a trivial result and is valid by construction;
- if $w_{ij} \to \bar{w} \land \sigma > 0 \Rightarrow \beta_{ij} = \frac{\beta + \delta_\beta}{2}$;
- if $w_{ij} \to \infty \land \sigma > 0 \Rightarrow \beta_{ij} = \beta$
- if $w_{ij} \to 0 \land \sigma > 0 \land \bar{w} >> 0 \Rightarrow \beta_{ij} = \delta_\beta$

As can be seen from Figure 3.15 as β changes, the times to infection generated by the distributions change. The same reasoning can also be extended to the δ and ϵ parameters. In the figure, two classic distributions

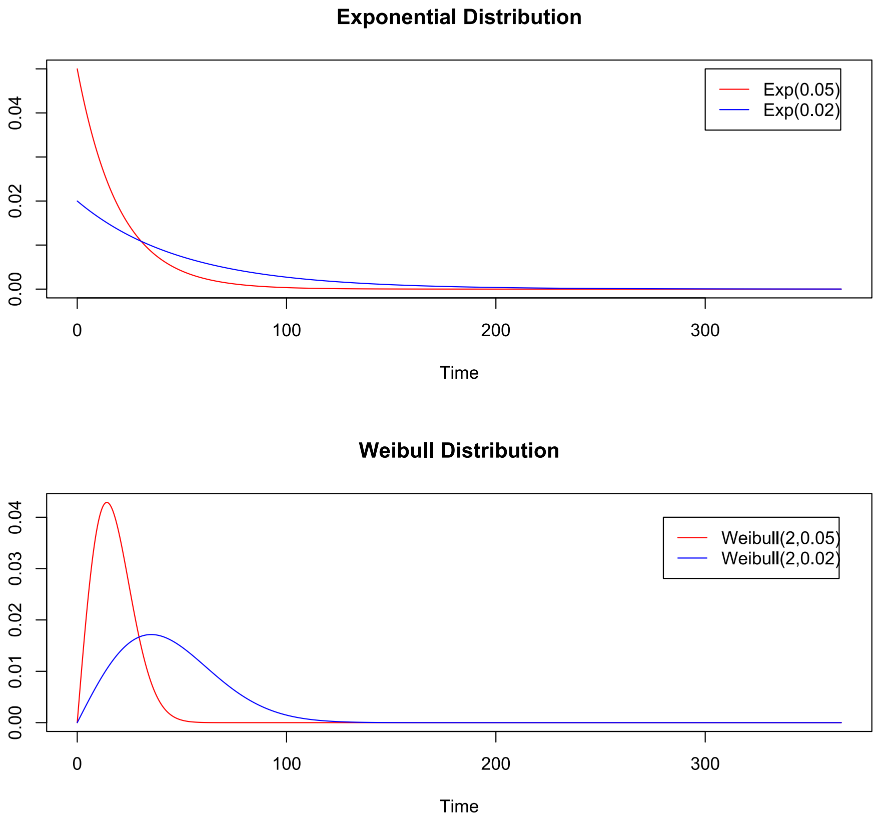


Figure 3.15: Exponential vs Weibull distributions

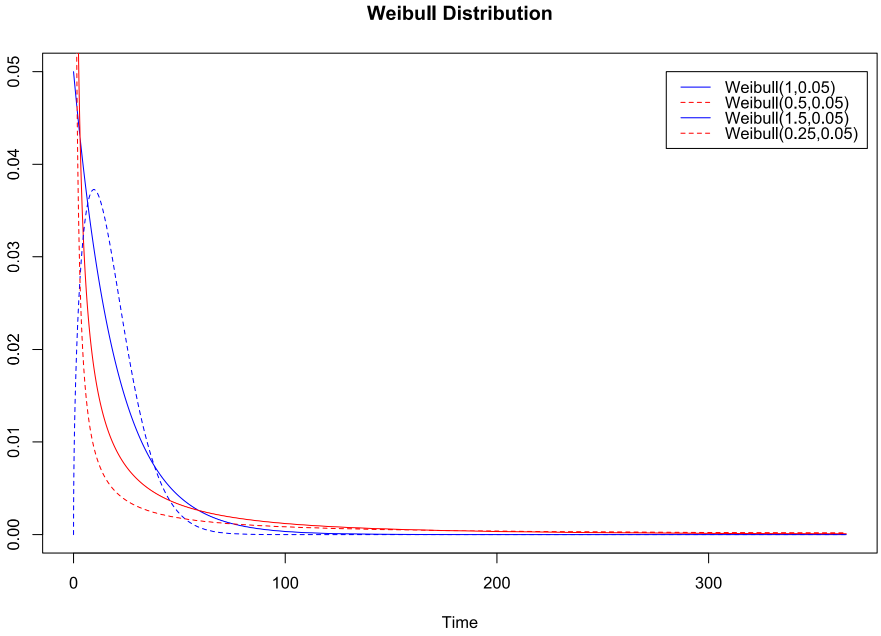


Figure 3.16: Weibull p.d.f. with different shape values.

have been taken into consideration to generate the times. The first is an exponential. It can be seen that as β decreases, the mean of the distribution increases and consequently the times to infection. The same reasoning applies to the Weibull distribution, which, unlike the exponential distribution, makes it possible to act not only on the mean but also on the *skewness* of the distribution by means of the `shape` parameter. This can be seen in Figure 3.16.

3.7 Weibull Distribution

In this section, the aim is to justify the use of the Weibull distribution to generate times to infection or times to recovery. The formulae that will be illustrated will apply in particular to infection times (and thus linked to the parameter β), but the same reasoning can be made for self infection times and recovery times (hence the ϵ and δ parameters).

Given a random variable $\tilde{X}$, it is distributed as a $Weibull(\alpha,\sigma)$ if it has the following probability density function (p.d.f.) and cumulative distribution function (c.d.f.):

$$f_{\tilde{X}}(x) = \left(\frac{\alpha}{\sigma}\right) \cdot \left(\frac{x}{\sigma}\right)^{\alpha-1} \cdot \exp\left\{-\left(\frac{x}{\sigma}\right)^{\alpha}\right\} \tag{3.58}$$

$$= \left(\frac{\alpha}{\frac{1}{\beta}}\right) \cdot \left(\frac{x}{\frac{1}{\beta}}\right)^{\alpha-1} \cdot \exp\left\{-\left(\frac{x}{\frac{1}{\beta}}\right)^{\alpha}\right\} = \tag{3.59}$$

$$= (\alpha\beta) \cdot (x\beta)^{\alpha-1} \cdot \exp\{-(x\beta)^{\alpha}\}, \quad x, \alpha, \beta, \sigma > 0 \tag{3.60}$$

$$F_{\tilde{X}}(x) = 1 - \exp\left\{-\left(\frac{x}{\sigma}\right)^{\alpha}\right\} \tag{3.61}$$

$$= 1 - \exp\left\{-\left(\frac{x}{\frac{1}{\beta}}\right)^{\alpha}\right\} \tag{3.62}$$

$$= 1 - \exp\{-(x\beta)^{\alpha}\}, \quad x, \alpha, \beta, \sigma > 0 \tag{3.63}$$

The parameter α is called *shape* parameter while the parameter σ is called *scale* parameter. They must both be greater than zero and the support $\mathcal{S}_{\tilde{X}}$ of the random variable $\tilde{X}$ is also defined in $[0, \infty]$. The Weibull distribution is much more flexible than the exponential distribution. It can also be seen from the c.d.f. that setting the alpha parameter equal to 1 leads back to the c.d.f. of an exponential distribution.

$$\mathbb{E}[\tilde{X}] = \sigma \cdot \Gamma\left(1 + \frac{1}{\alpha}\right) = \tag{3.64}$$

$$= \frac{1}{\beta} \cdot \Gamma\left(1 + \frac{1}{\alpha}\right) \tag{3.65}$$

$$\sigma^2\left(\tilde{X}\right) = \sigma^2\left[\Gamma\left(1 + \frac{2}{\alpha}\right) - \left(\Gamma\left(1 + \frac{1}{\alpha}\right)\right)^2\right] = \tag{3.66}$$

$$= \frac{1}{\beta^2} \cdot \left[\Gamma\left(1 + \frac{2}{\alpha}\right) - \left(\Gamma\left(1 + \frac{1}{\alpha}\right)\right)^2\right] \tag{3.67}$$

$$\gamma(\tilde{X}) = \frac{\Gamma\left(1 + \frac{3}{\alpha}\right) - 3\Gamma\left(1 + \frac{2}{\alpha}\right)\Gamma\left(1 + \frac{1}{\alpha}\right) + 2 \cdot \left(\Gamma\left(1 + \frac{1}{\alpha}\right)\right)^3}{\left[\Gamma\left(1 + \frac{2}{\alpha}\right) - \left(\Gamma\left(1 + \frac{1}{\alpha}\right)\right)^2\right]^{\frac{3}{2}}} \tag{3.68}$$

For the sake of simplicity, the formulas have also been given by replacing the parameter σ with $\frac{1}{\beta}$, as it is precisely the latter that will be used

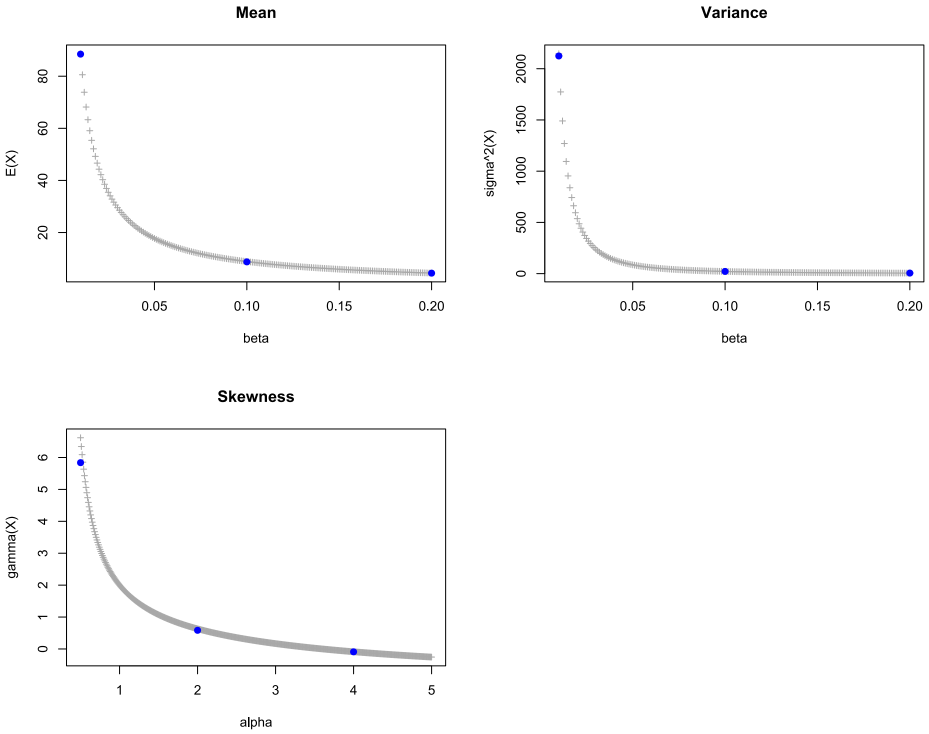


Figure 3.17: Movements of mean, variance and skewness as β and α change (In grey the exact quantities, in blue the simulated quantities).

for interpretation purposes in the $HG-SIS$ model. The same formulas can also be derived with the δ and ϵ parameter. From Equation 3.64 to Equation 3.68 it is also possible to see the formulae for the principal moments of the Weibull distribution, also as a function of beta.

From both the equations and Figure 3.17, it is possible to see the trends in mean, variance and skewness as the beta parameter changes. Specifically, it can be seen that as beta increases, both mean and variance tend to zero, while skewness is independent of the beta parameter. From a practical point of view, it can be deduced that choosing a very small beta (or delta or epsilon) in the parameterisation of the epidemic model will lead to large averages of the times to infection, but consequently also to greater variability in the simulations.

3.8 Cost and recovery functions

When a node (critical or non-critical) becomes infected or healthy again, the cost of the event must be calculated. In the case of loss due to infection (or self infection) of a single node, one must model the cost of the loss, which, depending on the contractual conditions of the policy one intends to price (and the information available) may cover the material damage to the PC, the damage to third parties, the economic cost due to the loss of data, etc. In the case of the recovery process, on the other hand, the loss is the cost necessary to re-establish the functionality of the node. It goes without saying that these costs vary widely depending on the type of information handled, the type of attack suffered, the sector of the company involved, etc. In this dissertation, the only important distinction made is between critical and non-critical nodes.

For non-critical nodes, it is essential to introduce the Beta distribution that is the foundation of both loss cost and recovery cost modelling.

Beta Distribution Beta distribution is widely used in the actuarial field. Its main characteristic is its limited positive support. In its classical formulation, the support of $\tilde{X} \sim Beta(a,b)$ is $\mathcal{S}_{\tilde{X}} \in (0,1)$. Thus, assuming that an object is insured for a monetary value of 1, the Beta distribution can be used to simulate the economic loss due to a claim. In this way, it will never be possible to obtain a claim greater than the insured object value itself.

$$B(a,b) = \int_0^1 t^{a-1}(1-t)^{b-1}dt = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)} \tag{3.69}$$

$$f_{\tilde{X}}(x) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} x^{a-1}(1-x)^{b-1}; \quad 0 < x < 1 \tag{3.70}$$

The following equation refers to the probability density function (p.d.f.) of the random variable $\tilde{X}$ distributed as a Beta of parameters a and b. Using the p.d.f., it is possible to derive the *moment* of order k of the random variable:

$$\mathbb{E}\left(X^k\right) = \int_0^1 x^k \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} x^{a-1}(1-x)^{b-1} dx \tag{3.71}$$

$$= \int_0^1 \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} x^{a+k-1}(1-x)^{b-1} dx \tag{3.72}$$

$$= \frac{\Gamma(a+k)}{\Gamma(a)} \frac{\Gamma(a+b)}{\Gamma(a+b+k)} \int_0^1 \frac{\Gamma(a+b+k)}{\Gamma(a+k)\Gamma(b)} x^{a+k-1}(1-x)^{b-1} dx \tag{3.73}$$

$$= \frac{\Gamma(a+k)}{\Gamma(a)} \frac{\Gamma(a+b)}{\Gamma(a+b+k)} \tag{3.74}$$

By replacing k with 1,2 and 3, it is possible to derive the expected value $\mathbb{E}(\tilde{X})$, variance $\sigma^2(\tilde{X})$, coefficient of variability $CV(\tilde{X})$ and skewness $\gamma(\tilde{X})$ of the random variable $\tilde{X}$. As can easily be seen, all these characteristics depend on both parameters, which are therefore crucial in the calibration phase.

$$\mathbb{E}(\tilde{X}) = \frac{a}{a+b} \tag{3.75}$$

$$\mathbb{E}\left(\tilde{X}^2\right) = \frac{a(a+1)}{(a+b)(a+b+1)} \tag{3.76}$$

$$\mathbb{E}\left(\tilde{X}^3\right) = \frac{a(a+1)(a+2)}{(a+b)(a+b+1)(a+b+2)} \tag{3.77}$$

$$\mathbb{E}(\tilde{X}) = \frac{a}{a+b} \tag{3.78}$$

$$\sigma^2(\tilde{X}) = \frac{ab}{(a+b)^2(a+b+1)} \tag{3.79}$$

$$CV(\tilde{X}) = \frac{\sigma(\tilde{X})}{\mathbb{E}(\tilde{X}} = \sqrt{\frac{b}{a(a+b+1)}} \tag{3.80}$$

$$\gamma(\tilde{X}) = \frac{2(b-a)\sqrt{a+b+1}}{(a+b+2)\sqrt{ab}} \tag{3.81}$$

It is possible, however, to obtain a random variable $\tilde{Y}$ in such a way that its support $\mathcal{S}_{\tilde{Y}} \in (0, w)$ is always defined positive, but is also greater than 1. When signing a policy, for example, one could insure each 'simple' node in the network up to a value of $1000 - 1500$ euros. In this way, in the event of infection, the loss would be superiorly limited thanks to the use of this Beta random variable. Below are the formulae of the probability density function (p.d.f.), cumulative distribution function (c.d.f.) and the main characteristics of $\tilde{Y}$ such as mean $\mathbb{E}(\tilde{Y})$, variance $\sigma^2(\tilde{Y})$, coeffient of volatility $CV(\tilde{Y})$ and skewness $\gamma(\tilde{Y})$.

$$\tilde{Y} = w \cdot \tilde{X} \tag{3.82}$$

$$\mathcal{S}_{\tilde{Y}} = (0, w) \tag{3.83}$$

$$f_{\tilde{Y}}(y) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} \left(\frac{y}{w}\right)^{a-1} \left[1 - \left(\frac{y}{w}\right)\right]^{b-1} \frac{1}{w} \quad 0 < y < w \tag{3.84}$$

$$= \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} \frac{1}{w^{a+b-1}} y^{a-1} (w-y)^{b-1} \tag{3.85}$$

$$F_{\tilde{Y}}(y) = \int_0^{\frac{y}{w}} \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} t^{a-1}(1-t)^{b-1} dt \quad 0 < y < w \tag{3.86}$$

$$E\left(Y^k\right) = w^k E(X) \tag{3.87}$$

$$\mathbb{E}(\tilde{Y}) = w \frac{a}{a+b} \tag{3.88}$$

$$\sigma^2(\tilde{Y}) = w^2 \frac{ab}{(a+b)^2(a+b+1)} \tag{3.89}$$

$$CV(\tilde{Y}) = \sqrt{\frac{b}{a(a+b+1)}} \tag{3.90}$$

$$\gamma(\tilde{Y}) = \frac{2(b-a)\sqrt{a+b+1}}{(a+b+2)\sqrt{ab}} \tag{3.91}$$

It is interesting to note that characteristics such as the coefficient of variability and skewness are independent of the parameter w (upper extremity of the support). Obviously, other distributions for "simple" nodes could also be used in the pricing phase and provide for maximum limits as well as deductibles.

Cost and recovery function for non-critical nodes As a further customisation to model the loss due to infection of a common node [30] introduced *cost and recovery functions*. The former depends only on the loss l_v and an arbitrarily chosen parameter c, while the latter is a function of the node's initial wealth (e.g. 1000–1500 euros, consistent with the chosen Beta distribution parameters) and the recovery time r_v required to re-establish functionality. Also in this case, there are two arbitrarily chosen parameters c_1 and c_2.

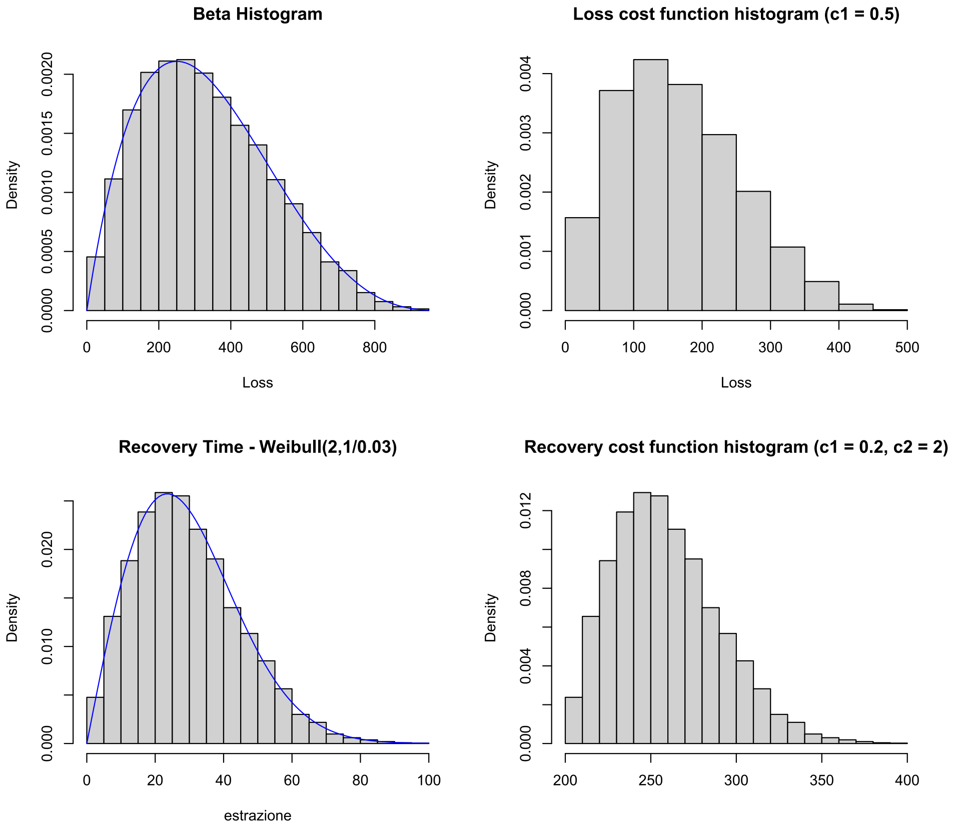


Figure 3.18: Histograms of cost and recovery functions.

$$\eta_v(l_v) = c \cdot l_v \tag{3.92}$$

$$\rho_v(w_v, r_v) = c_1 \cdot w_v + c_2 \cdot r_v \tag{3.93}$$

In the Figure 3.18 the histograms of the loss $\tilde{L}_v$ and the cost function η_v using a parameter $c = 0.5$ can be seen. As can be seen, having chosen a very simple cost function in this case, it maintains the *shape* of the distribution and positive skewness. Even by generating recovery times with a Weibull of parameters 2 and 1/0.03, it is possible to obtain the histogram of the recovery cost function. Again, it can be seen that the simplicity of the function chosen retains the shape of the starting distribution. In both cases, these are simple linear transformations of random variables.

Cost function for critical nodes - LogNormal Distribution For criticals nodes (such as servers, particularly critical and sensitive computers, databases, etc.) a different claims distribution was chosen. The underlying rationale is that in this case there is not only a problem of the cost of the attacked device, but of damage to third parties, reputational damage etc. Think of the case where the system that runs the production machinery in a manufacturing company goes down. In this case, it would no longer be a problem of the device of the single employee who would be unable to work, but it would be a problem that would have much wider and more difficult consequences to solve.

As will also be seen in the next section of this dissertation, critical nodes will be more difficult to infect than "common" nodes, but they will also have a much, much longer recovery time, precisely because it is often necessary to call in third-party assistance and, in the case of e.g. data encryption due to a ransomware attack, the critical node's "recovery" time can be longer. A single cost and recovery function was chosen, which is based on the *Lognormal* distribution. In the following Equations, one can see the probability density function (p.d.f.) and cumulative distribution function (c.d.f.) of a random variable $\tilde{Y}$ such that the logarithm of $\tilde{Y}$ is distributed as a Normal with mean μ and variance σ^2:

$$f_{\tilde{X}}(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad -\infty < x < \infty, \quad \text{Normal} \tag{3.94}$$

$$f_{\tilde{Y}}(y) = \frac{1}{y\sigma\sqrt{2\pi}} e^{-\frac{(\log(y)-\mu)^2}{2\sigma^2}} \quad 0 < y < \infty, \quad \text{Lognormal} \tag{3.95}$$

$$F_{\tilde{Y}}(y) = \int_0^y \frac{1}{t\sigma\sqrt{2\pi}} \mathrm{e}^{-\frac{(\log(t)-\mu)^2}{2\sigma^2}} dt \tag{3.96}$$

Using the generating function of the moments $M_{\tilde{Y}}(t)$ and cumulants $\Psi_{\tilde{Y}}$ of the random variable $\tilde{Y}$, it is possible to derive the main characteristics of this variable such as mean $\mathbb{E}[\tilde{Y}]$, variance $\sigma^2(\tilde{Y})$, standard deviation $\sigma(\tilde{Y})$, coefficient of variation $CV(\tilde{Y})$ and skewness $\gamma(\tilde{Y})$:

$$\alpha_t = \mathbb{E}(\tilde{Y}^t) = \mathrm{e}^{\left[\mu t + (1/2)\sigma^2 t^2\right]} \tag{3.97}$$

$$\mathbb{E}(\tilde{Y}) = \mathrm{e}^{\left[\mu + \frac{\sigma^2}{2}\right]} \tag{3.98}$$

$$\sigma^2(\tilde{Y}) = \mathrm{e}^{\left[2\mu + 2\sigma^2\right]} - \mathrm{e}^{\left[2\mu + \sigma^2\right]} = \left(\mathrm{e}^{\sigma^2} - 1\right)\mathrm{e}^{\left[2\mu + \sigma^2\right]} \tag{3.99}$$

$$\sigma(\tilde{Y}) = \sqrt{\mathrm{e}^{\sigma^2} - 1}\,\mathrm{e}^{\left[\mu + \frac{1}{2}\sigma^2\right]} = \sqrt{\mathrm{e}^{\sigma^2} - 1}\,E(Y) \tag{3.100}$$

$$CV(\tilde{Y}) = \sqrt{\mathrm{e}^{\sigma^2} - 1} \tag{3.101}$$

$$\gamma(\tilde{Y}) = CV(\tilde{Y})(3 + CV(\tilde{Y})^2) \tag{3.102}$$

These characteristics are essential when calibrating the model and pricing the policy. Indeed, the insurer will have to choose which mean to give to the distribution, as well as the variance, etc. This is not easy as these values clearly depend on the sector of the company to be insured, its size, resilience to cyber risk and many other factors.

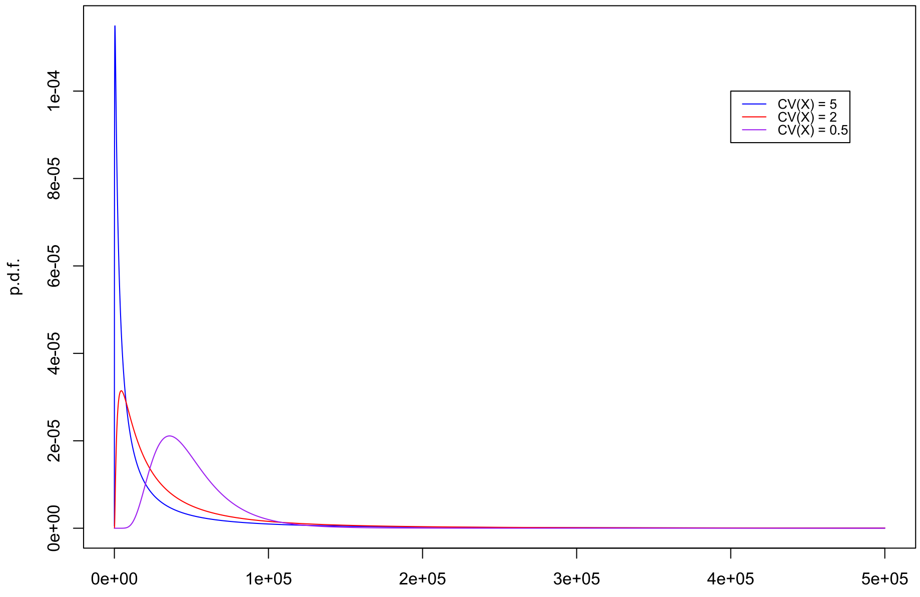


Figure 3.19: Different p.d.f. of a lognormal distribution as the coefficient of variation changes.

As can be seen from Figure 3.19, the choice of the parameters of a lognormal distribution has a great impact on its distribution and its tail. Indeed, it is well known from actuarial theory that such a distribution (or Gamma distribution or Pareto distribution) is used when one wants to model the loss of very long-tailed claims. The Figure shows how the $CV(\tilde{X})$ of the distribution affects its variance and skewness.

Normally in an insurance contract there are policy limits and deductibles. In a somewhat simplified way, a *truncated lognormal distribution* can be used. In this way, by setting a ceiling, it is possible to simulate claims that never exceed that ceiling and thus influence the overall premium, which would decrease.

3.9 The simulation Algorithm

The model used for the simulations in this dissertation is an inspiration from the Non-Markov model of [30] and the $HG-SIS$ model of [31] with appropriate distinctions between critical and non-critical nodes.

The objective is to simulate the *cumulative loss* during the entire time span of the insurance contract. For each node v and at each time instant t, it is in fact possible to calculate:

$$s_v(t) = \sum_{\ell=1}^{M_v(t)} \left[\eta_v(L_{v,\ell}) + \rho_v(W_v, R_{v,\ell})\right] \tag{3.103}$$

where η_v is the cost function due to infection (or self infection), ρ_v is the recovery process function, L_v is the node loss, W_v is the initial wealth of the node and R_V is the length of the service slowdown. In this way, at time instant t, the cumulative loss of node v can be calculated, summing up the total number of infections of node v up to time instant t: $M_v(t)$.

Then considering all nodes and summing up the cumulative loss up to instant t for all nodes in the network, one obtains:

$$S(t) = \sum_{v=1}^{N} s_v(t) = \sum_{v=1}^{N} \sum_{\ell=1}^{M_v(t)} \left[\eta_v(L_{v,\ell}) + \rho_v(W_v, R_{v,\ell})\right] \tag{3.104}$$

In Altorithm 1 one can see the behaviour of the algorithm. First it starts with the network dataset where all the main information is available: the group to which a node belongs, the distinction between critical and non-critical nodes, the node ID and in general all possible attributes of the nodes. Next the number of simulations to be carried out is needed, the parameters required for the distributions such as the beta matrix (in the case of the HG-SIS model), the deltas and epsilons distinguished for critical and non-critical nodes. In order to calculate the loss due to infection and the loss in the event of recovery, the parameters of the relevant distributions, distinguished for critical and non-critical nodes, are also required. The underlying rationale is simple, an attempt is made to simulate recovery times (for infected nodes at a given time instant) and infection and self-infection times for all others. Then one sees which event happens before the others and increases the time for that minimum time instant. If the first event to occur is a recovery time then the status of the corresponding node is changed and the loss is calculated using the appropriate recovery function. Conversely, if an infection (or self infection) occurs, the loss is calculated with the appropriate cost function, remembering to distinguish between critical and non-critical nodes.

For each secure node, the infected neighbours must always be identified and, by summing up the betas in the row corresponding to the node under examination and in the columns corresponding to the IDs of the infected neighbours, the time of self-infection is simulated from a Weibull. In this way there is a double effect taken into account. The times to infection will be the lower the greater the weight between a node and the infected neighbour, since the sigmoidal transformation of the betas takes place, and the greater the number of infected neighbours, the lower the times to infection. In fact, as can be seen in the Equation 3.105 and in the Figure 3.20, by adding up more beta values (in the figure it is assumed that all betas are equal) the times to infection on average decreases.

Alternatively, instead of summing up the betas and generating a single infection time for a given node, it is possible to generate as many times as there are infected neighbours. In this way, however, it is difficult to take into account the quantity of infected neighbours because times of practically the same distribution would be simulated. In reality, the probability of infection is probably as great as the number of infected devices with which one communicates. It is true, however, that at least in [31] the beta transformation was introduced to at least take into account the Graph Mining Approach and thus the intensity of connection between nodes. In general, it can be appreciated that the network topology has a great effect on the probability of infection, because the more interconnections in the network, the greater the probable infected neighbours and thus the lower the times to infection for each individual node. Conversely, the self-infection times are independent of the network topology, and only the calibration of the parameters required for the chosen distribution is essential.

From a theoretical point of view, with this algorithm it is possible to 'snapshot' the network situation and infections at each time step of the algorithm. From a practical point of view, if the network is very large, this results in a very onerous amount of information. For pricing purposes, it is only necessary to store the cumulative loss per node distinguished between recovery and loss cost for normal nodes and only loss cost for critical nodes. In fact, it should be remembered that for critical nodes, a long-tail distribution such as lognormal, Gamma or Pareto is used, which also includes recovery costs. In the case of recovery of a critical node, therefore, only the status of the node is changed from 1 to 0 in the algorithm.

$$\hat{\beta}_\ell = \beta_{\ell,1} + \beta_{\ell,2} + \cdots + \beta_{\ell,D_\ell} \tag{3.105}$$

The distributions chosen, the parameters required and their calibration are essential in an algorithm such as the one presented. Computational times can increase dramatically if one increases the size of the network and chooses distributions such that, by minimising the times to recovery/infection, one moves infinitesimal fractions of a day in the algorithm and simulating all events over the course of a year becomes too onerous. What is important is to identify the relevant events that lead to material damage. For this reason, as will be seen in the following chapter, parameters were chosen that provide plausible results and simulation times that are compatible with equipment that is not particularly powerful.

Algorithm 1 Simulation of a one year contract using and HG-SIS model

```
Require: Infection rate matrix $\mathbf{B}$, initial status of all nodes, number of simulations $n_{sim}$, duration of the contract $T$, number of groups $G$, critical flag
  for i = 1 to $n_{sim}$ do
    while $t \leq T = 365$ do
      Calculate the number of infected nodes $n_{infected,t}$ at time $t$ and find their ID
      Calculate the number of secure nodes $n_{secure,t}$ at time $t$ and find their ID
      Generate random recovery time $r_1, r_2, \dots, r_{n_{infected,t}}$ according to a Weibull of parameters $\alpha_\delta$ and $\delta$
      for $v \in$ secure nodes $n_{secure,t}$ do
        Determine the infected neighbours and their ID of node $v$ $j_1, j_2, \dots, j_{d_v}$ where $d_v$ is the number of infected neighbours of node $v$ at time $t$
        Sum the corresponding $\beta$ of infected neighbours
        Check whether node $v$ is critical or not
        Generate random infection time according to a Weibull of parameters $\alpha_\beta$ and $\beta_\Sigma$. If critical use $\alpha_{\beta_{critical}}$ otherwise use $\alpha_\beta$
        Depending on whether node $v$ is critical or not, it calculates the self infection time according to a Weibull of parameters $\alpha_\varepsilon$ and $\varepsilon$ or $\alpha_{\varepsilon_{critical}}$ and $\varepsilon_{critical}$.
        Determine the shortest time for each node $v$ between infection time and self-infection time: $\ell_v$
      end for
      Determine time for the first event: $t_1 = \min\{r_1, r_2, \dots, r_{n_{infected,t}}, \ell_1, \dots, \ell_{n_{secure,t}}\}$
      if infection occurs then
        Change status from 0 to 1 and calculate the loss (based on whether the corresponding node is critical or non-critical)
      else
        Change status from 1 to 0 and calculate the loss (based on whether the corresponding node is critical or non-critical)
      end if
      $t = t + t_1$
    end while
    Return: t, network status, cumulative loss for every node
  end for
  Output: final status of every node and cumulative loss for every node.
```

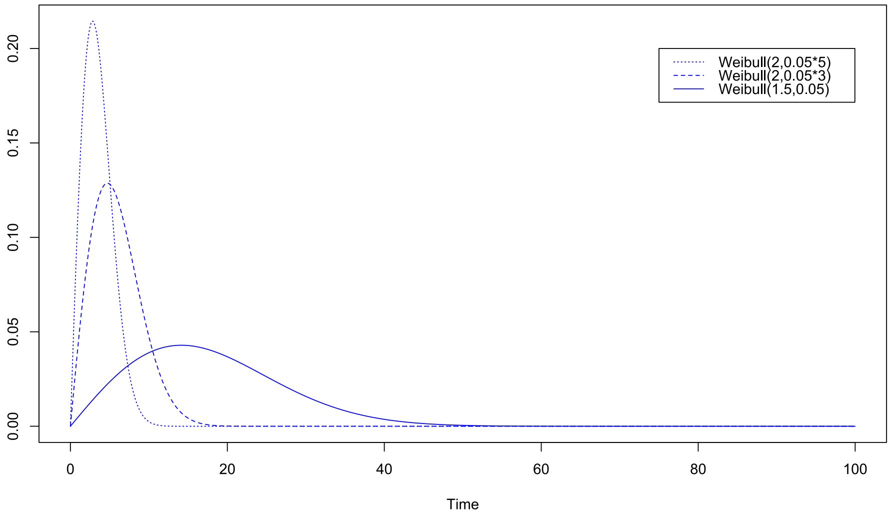


Figure 3.20: Weibull p.d.f. with different scale values.

Premium Calculation Calculation of the premium. It was mentioned earlier that the objective of the Algorithm 1 is to identify the loss cumulated for all nodes in the network considered $S(T)$. This quantity can also be regarded as a random variable $\tilde{S}(T)$ and, from a premium calculation perspective, it is essential to identify the *risk premium* i.e:

$$\mathbb{E}[\tilde{S}(T)] \tag{3.106}$$

The risk premium is in fact the expected value of the overall compensation to be paid by the insurer over the coverage period. Adding the *safety loadings* to the risk premium gives the *pure premium*.

$$P = \mathbb{E}[\tilde{S}(T)] + \text{safety loadings} \tag{3.107}$$

This is the global compensation transferred to the insurer. Safety loadings are widely used in actuarial and pricing. It reflects the inherent riskiness of the insurance transaction and is a kind of risk premium, but also reflects the remuneration of the cost of capital.

Safety loading is intrinsically linked to the cost of capital since, due to the Solvency II directive, the higher the riskiness of the LoB considered, the higher the capital requirement and thus the higher the safety loading. Adding expense loading to the pure premium gives the tariff premium. This is because the insurance company charges the insured. These include acquisition expenses, collection expenses and management expenses. Consequently, the premium actually paid is the risk premium, safety loadings, expense loadings, taxes and any other charges that may be imposed on the policy.

In this dissertation, only the risk premium and the pure premium will be calculated. This is because expense charges are very entity specific and depend on the sales channel of the policies, whether the policy in question is compulsory or not, whether it is single premium or regular premium etc. In addition, there are fees that can be considered as an exogenous variable and therefore out of scope. Two approaches will be used to calculate the pure premium. The first is the standard deviation principle:

$$P = \mathbb{E}[\tilde{S}(T)] + \alpha \cdot \sqrt{\sigma^2(\tilde{S}(T))} \tag{3.108}$$

Basically, the remuneration for risk is proportional (α) to the standard deviation of the total cost of claims random variable during the policy coverage period. Note that from a theoretical point of view alpha can also be negative. Consider the case where an insurance company wants to gain market share by applying discounting. It is then possible that for limited periods of time a negative safety loading is applied. A second approach is to consider the $60-70$th percentile of the total claims cost distribution. In case of positive skewness of the distribution the $60-70$th percentile would be higher than the average of the distribution.

In the next Chapter two case studies will be analysed.

Chapter 4

Two case studies

In this chapter, two case studies are analysed and commented on in order to better summarise and exemplify what was explained in the previous chapter. The focus is on small-medium sized companies, since, as explained before, the algorithm is onerous in terms of computational time.

4.1 Case Study 1

The first case study is relatively simple. It consists of a network of 77 nodes of which 75 "simple" nodes and 2 critical infrastructures. Following the approach described in the previous chapter, given certain desired characteristics, the network was created. The `make_a_graph` function was used, using the parameters shown below.

```
G <- make_a_matrix(num_groups = 3,
                   size_group = 25,
                   p_within = 0.8,
                   p_between = 0.01,
                   num_criticals = 2,
                   p_criticals = 0.1,
                   overlapping = FALSE,
                   intensity_overlapping = 0,
                   overlapping_quota = 0)
```

The 75 simple nodes are distributed in 3 clusters/groups of 25 nodes

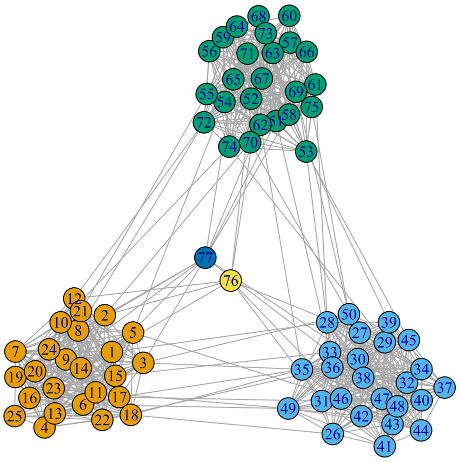


Figure 4.1: Case Study 1 - Network plot

each. The clusters are internally connected with a probability of 0.8 and between distinct clusters the connections have a probability of 0.01.

Critical nodes, on the other hand, are connected to other nodes with a probability of 0.1. As can be seen in the Figure 4.1, the graph reflects the parameters chosen *a-priori*. At first glance, it can be seen that there is much communication within the same group and much less between distinct groups. , there is no overlapping of clusters in the network. At this point, however, the graph is still undirected and *unweighted*, so the connection between two nodes does not reflect the intensity of the connection itself. By definition, two nodes are connected if during a time span e.g. the last year, they have been the subject of at least one communication with each other.

In the Figure 4.1, the numbers represent the (unique) IDs of the nodes, while the different colours reflect the group membership that is used as an attribute of the node.

As was explained in the previous chapter, in order to be able to apply an $HG-SIS$ epidemiological model and replicate an infection dynamic, it

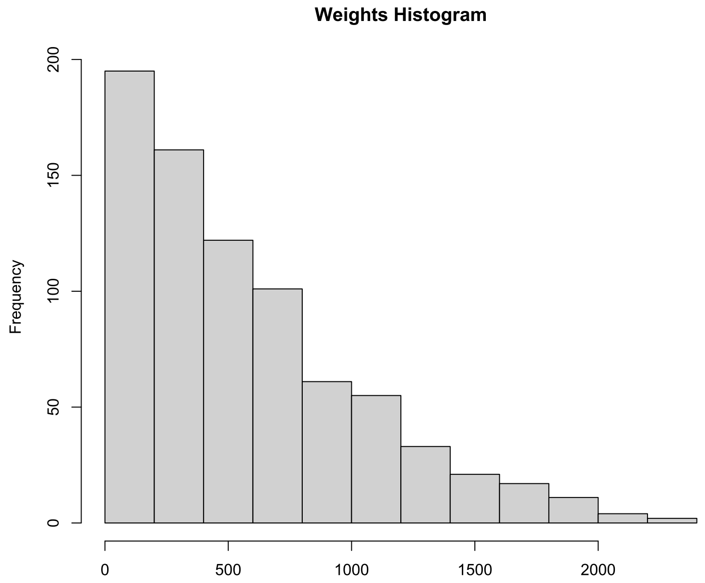


Figure 4.2: Case Study 1 - Weights histogram

is necessary to use a weighted network. Therefore, using an arbitrary assumption of on average $20 \cdot$(number of nodes) number of communications per day to be distributed for all edges and using a Negative Binomial distribution the weights for each edge of the network were obtained. Obviously, the minimum weight is 1, since there must have been at least one communication to be connected. The histogram of the weights of the network under consideration is shown in Figure 4.2. As can be seen, only a small proportion of the edges have a very high weight. This is due to the strong positive *skewness* of the distribution.

Once the weights have been obtained, these can be used in the phase of choosing the parameters of the distributions for the times to infection. 7 inputs are needed in the case where there is no critical infrastructure and 14 inputs in the other case. Table 4.1 shows the parameters used in Case Study 1. As there are two parameters for non-critical betas and as many for critical nodes. Furthermore, the parameters for critical infrastructures are smaller and therefore imply longer times to infection and self-infection than for normal nodes. In addition, the times to recovery

Table 4.1: Case Study 1 - Parameters

β	0.03	$\beta_{critical}$	$\beta/2$
$lower_{\beta}$	0.01	$lower_{beta_{critical}}$	$lower_{\beta}/2$
ε	0.01	$\varepsilon_{critical}$	$\varepsilon/3$
δ	0.1	$\delta_{critical}$	$\delta/1.5$
α_{β}	3	$\alpha_{\beta_{critical}}$	3
α_{ε}	3	$\alpha_{\varepsilon_{critical}}$	3
α_{δ}	3	$\alpha_{\delta_{critical}}$	3

and to re-establish node functionality are also longer. They can be parameterised according to the needs of the insurer and can be entity specific. The other parameters are the parameters needed for the Weibull distribution and a value of 3 allows for a somewhat less symmetric distribution. As an alternative, one can use only 8 parameters and replace the Weibull distribution with the Exponential distribution.

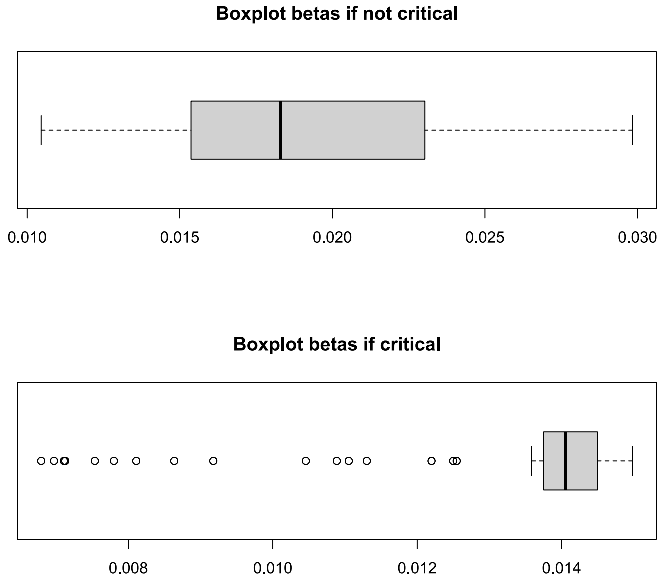


Figure 4.3: Case Study 1 - Betas boxplot

Once the lower and upper limits of beta have been determined, it is possible to apply the sigmoidal transformation described in the previous chapter and thus obtain a beta for each "1" in the adjacency matrix. Once all betas required for the chosen epidemiological model have been calculated, one can observe the respective boxplots in Figure 4.3. As can be seen, they reflect the desired properties of the sigmoidal transformation. They lie between a minimum and a maximum and vary with the respective weight of the edge considered.

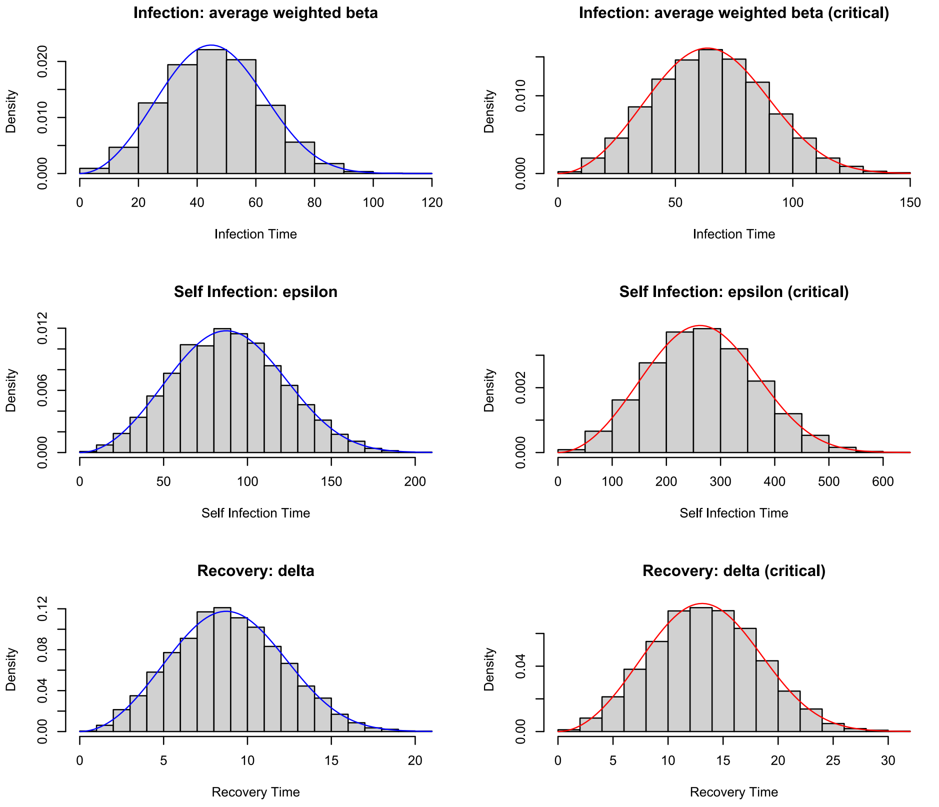


Figure 4.4: Case Study 1 - Beta, delta and epsilon time-distributions

In Figure 4.4, on the other hand, one can see the consequences of the chosen parameters in the form of histograms of infection times. For the betas, the average of the betas obtained by the sigmoidal transformation was used for convenience. Clearly, what is of interest in Algorithm 1 is to minimise all the times generated by the distributions, and consequently the left tail of the distributions considered is of interest.

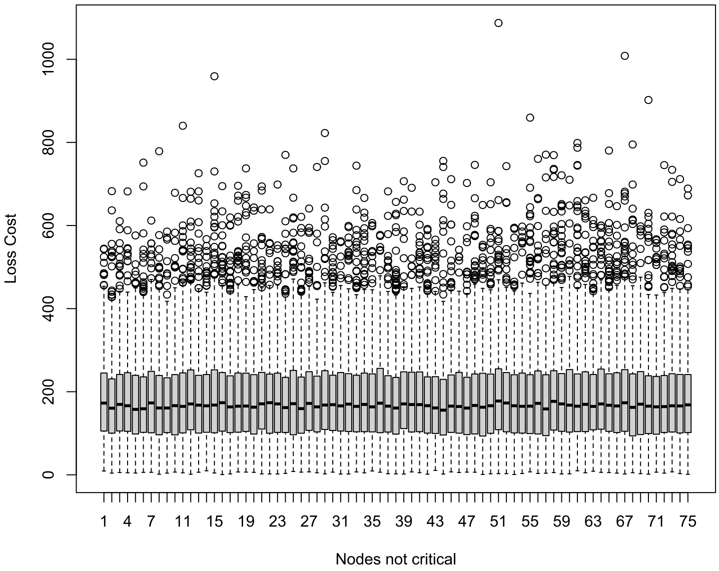


Figure 4.5: Case Study 1 - Boxplot of loss cost if node not critical

The results were then analysed. What is interesting from the point of view of policy pricing are the claims costs. Loss costs and recovery costs for non-critical nodes can be seen in Figure 4.5 and in Figure 4.6. Cost functions equal to:

$$\eta_v(l_v) = 0.5 \cdot l_v$$
$$\rho_v(w_v, r_v) = 0.2 \cdot 1000 + 2 \cdot r_v$$

and using an initial wealth for each node of EUR $1,000$. The distribution chosen for normal nodes is the 4-parameter Beta distribution. As can be seen from the graph, it is not uncommon for nodes to have had more than one infection during the policy's period of coverage, and consequently damage may be even greater than the node's initial wealth, even using a c parameter of 0.5. With regard to the boxplots per non-critical node in relation to the recovery cost, what should be noted is the proportionality of the recovery cost to the number of days required for recovery function. In this case, a clear distinction can be seen based on $1, 2, \dots$ recovery days respectively. Again, all parameters are customisable and can also be calibrated on the basis of the resilience of the company in question.

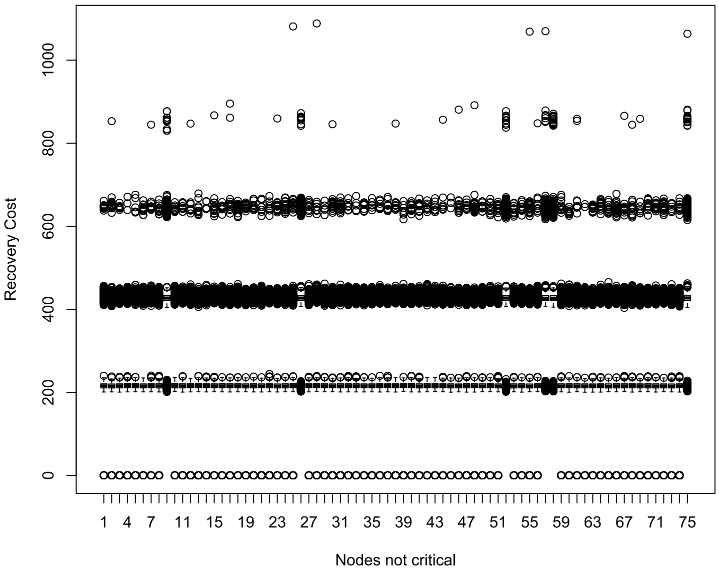


Figure 4.6: Case Study 1 - Boxplot of recovery cost if node not critical

A single cost/recovery function was chosen for critical infrastructures. When a critical node is infected, the algorithm extracts from a truncated log-normal the cost of the damage in the form of damage to third parties, material damage, etc., also including the recovery cost to return the critical infrastructure to full functionality. This distribution was chosen because there are usually maximum limits in the insurance contract for this type of damage and there is in any case an important tail of the distribution. In fact, it can be seen from Figure 4.7 that in the two boxplots of critical infrastructures, there is an average of around EUR 50k (as set by the input), but there are also some very extreme values (around the maximum limit chosen by the policy (EUR 500k).

The long tail chosen for critical infrastructure and the support of the distribution chosen has a strong influence on the final distribution of the aggregate cost of claims. In fact, as can be seen from Figure 4.9, most of the time there is a limited monetary amount of claims, even when many nodes are infected, because these are "common" nodes and may not give

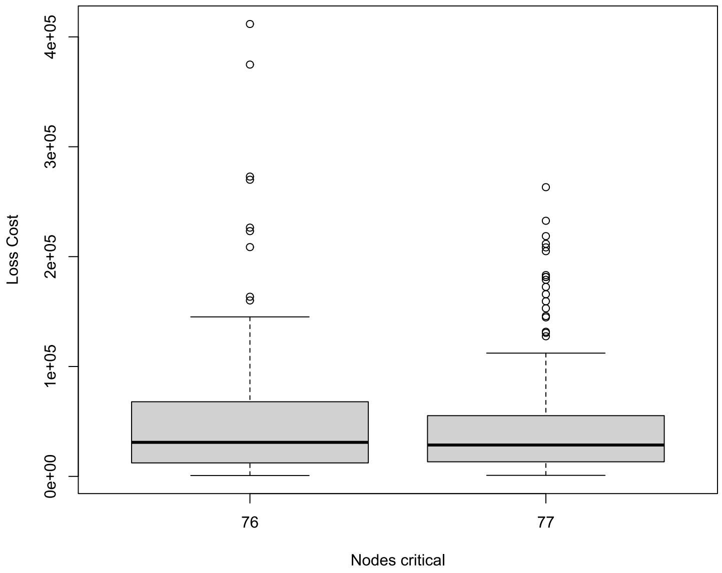


Figure 4.7: Case Study 1 - Boxplot of loss cost if node critical

rise to particularly important damage. It only takes a few critical physical infrastructures (2 out of 77 i.e. 2.6% of nodes) to have a potential loss of up to half a million. In the two pictures, in fact, one can see the same graph divided into the case where the total cost is less than EUR 50k and the case where that amount is greater. It should also be noted that *truncated* log-normal limits the insurer's losses only from the perspective of the individual claim. If, however, a node is infected several times or more than one critical infrastructure is infected during the contract term, it is possible to have an aggregate loss cost even greater than the single loss limit. In insurance practice, maximum limits are usually introduced for the aggregate cost of claims during the policy period, or *ad hoc* reinsurance contracts are entered into to limit possible exposures.

Since the total cost of claims is given by both infections of common nodes and infections of critical nodes, it is of interest to the insurer to identify what kind of distribution is obtained by mixing the source distributions. The distribution can be investigated using the `plotdist` function in the `R` package `fitdistrplus`. This function allows two empirical

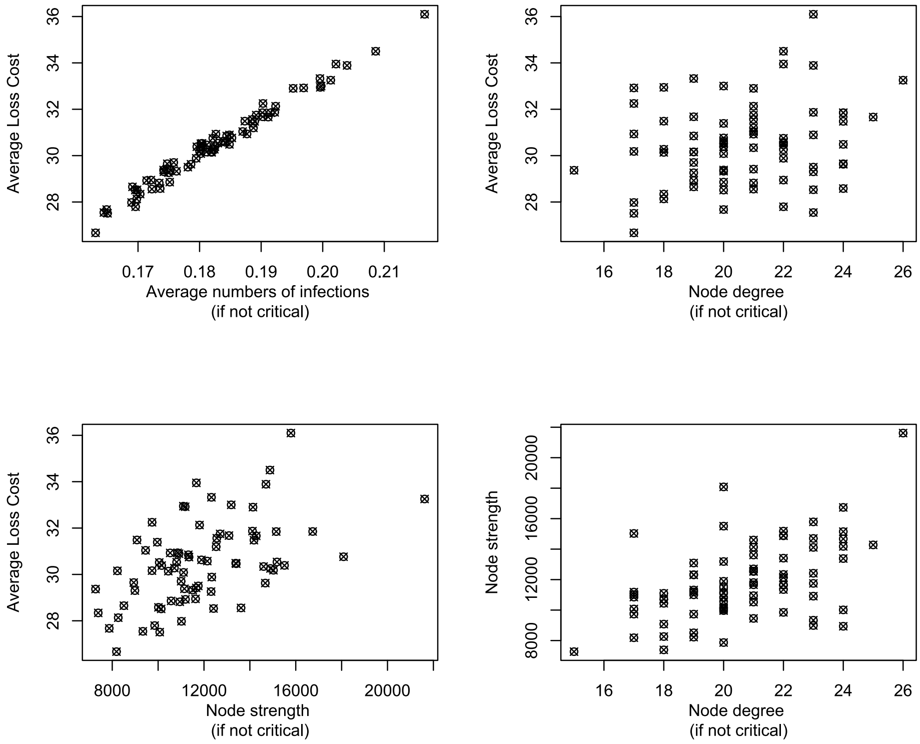


Figure 4.8: Case Study 1 - Some summary graphs

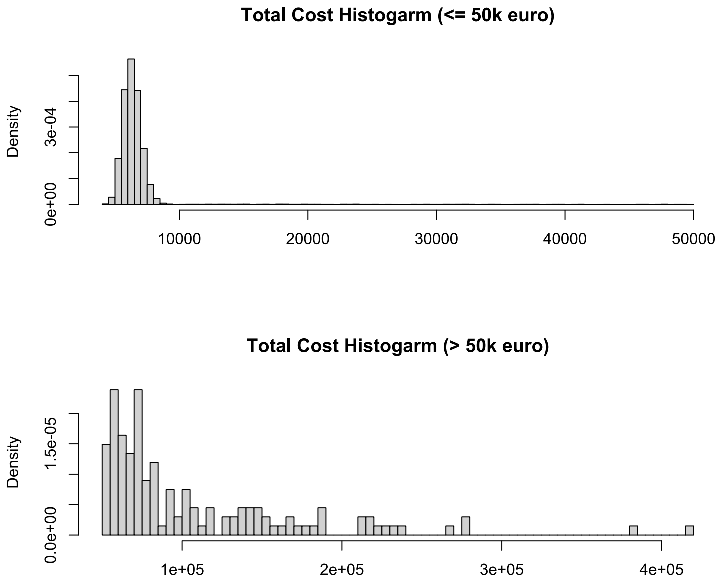


Figure 4.9: Case Study 1 - Total cost histogram

plots to be obtained. Figure 4.10 shows the result of the function applied to the simulation results of the network from Case Study 1. On the left is the histogram of the empirial density, on the right is the empirical cumulative distribution function (CDF). In addition, descriptive statistics such as skewness and kurtosis can be investigated. This helps to understand the symmetry/asymmetry of the distribution and the influence of the tail, which is also very important for capital requirement purposes for the insurer and for measuring risk more generally. From the statistics literature, however, it is known that skewness and kurtosis are not robust statistics. It is therefore necessary to use other techniques (such as bootstrapping) to try to relate the simulation results to a known distribution. Figure 4.11 shows the Cullen and Frey (1999) method applied to the total claims cost distribution. In this figure, the (non-parametric) bootstrapping methodology is used to try to bring the skewness and kurtosis of the simulated distribution back to known values.

Interpreting the resulting graph, one can see that, for the insurer, it is possible to estimate the total aggregate distribution using a Beta dis-

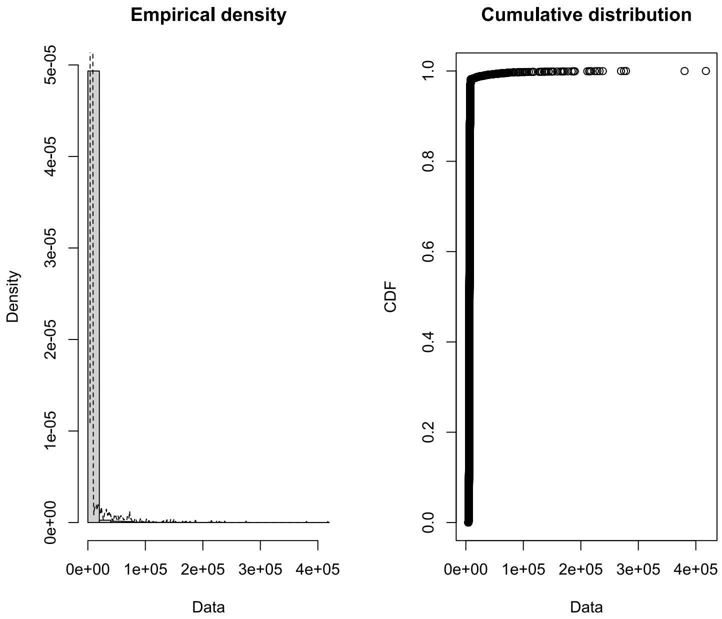


Figure 4.10: Case Study 1 - Empirical density and cumulative distribution of Total cost

tribution or even a Gamma distribution. Once the distribution has been identified, in order to calculate the insurance premium, it is necessary to calculate the expected value of the distribution and its standard deviation. Alternatively, the $60-70th$ percentile of the distribution can be calculated. In Case Study 1, the following results were obtained:

$$\mathbb{E}[\tilde{X}] = 7,225.38 \tag{4.1}$$

$$\mathbb{E}[\tilde{X}|\text{critical}] = 48,906.96 \tag{4.2}$$

$$\sigma(\tilde{X}) = 10,070.99 \tag{4.3}$$

$$\text{median}(\tilde{X}) = 5,256.39 \tag{4.4}$$

$$p_{70\%}(\tilde{X}) = 5,655.07 \tag{4.5}$$

$$p_{99.5\%}(\tilde{X}) = 61,705.06 \tag{4.6}$$

As can be seen from the results, the average aggregate cost of claims was EUR 7,225.38, driven by critical infrastructure claims. As can be seen from

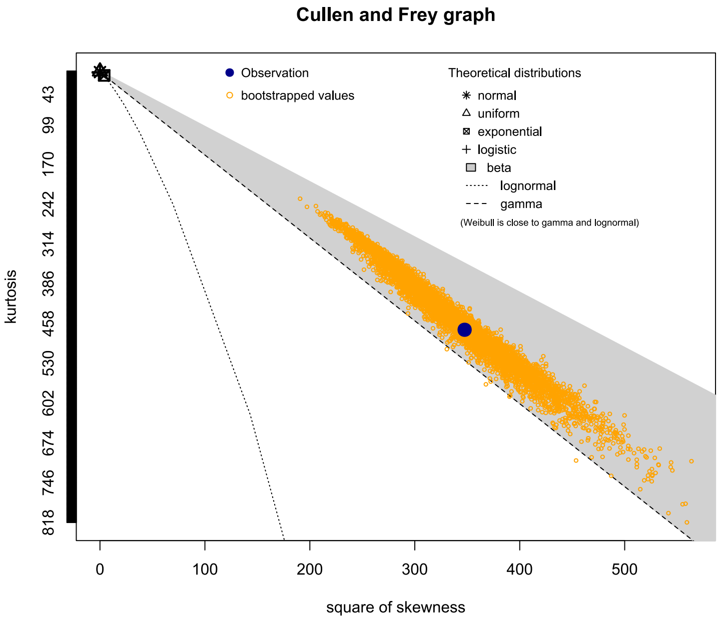


Figure 4.11: Case Study 1 - Cullen and Frey Plot of Total cost

the percentile values, a much larger than average amount is needed to cover expected losses in 99.5% of cases. The insurer can calculate the premium as a function of the risk premium $\mathbb{E}[\tilde{X}]$ and statistics such as standard deviation $\sigma(\tilde{X})$ or skewness $\gamma(\tilde{X})$. Alternatively, quantiles can be used. It is necessary that in addition to the risk premium there is a remuneration for the risk (safety loading), as explained in the previous chapter.

4.2 Case Study 2

In the second case study analysed in this dissertation, most of the layout of Case Study 1 was kept unchanged, while modifying specific (topological) characteristics of the network and infection dynamics.

```
G <- make_a_matrix(num_groups = 5,
                   size_group = 15,
                   p_within = 0.8,
                   p_between = 0.2,
                   num_criticals = 2,
                    p_criticals = 0.1,
                    overlapping = TRUE,
                    intensity_overlapping = 0.6,
                    overlapping_quota = 0.1)
```

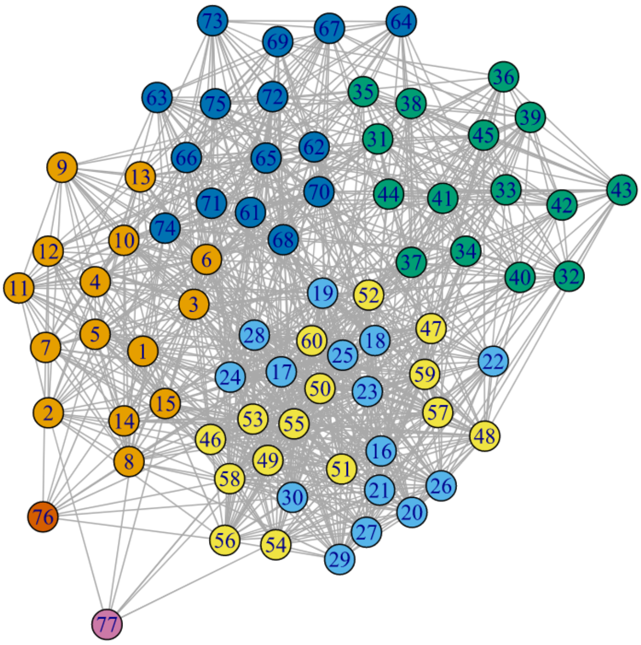


Figure 4.12: Case Study 2 - Network Plot

Topologically, the number of groups was increased while keeping the total number of nodes unchanged, from 3 to 5 groups. In addition, the communication/connection probability between distinct groups was increased and finally, overlapping between groups was also introduced. As can be seen from Figure 4.12, the groups can still be distinguished by a different colour and the two critical infrastructures with an ID of 76 and 77 respectively can be clearly distinguished.

The logic behind this choice of network is that as the number of connections increases, the infection dynamics should tend towards a higher number of infections and thus at least a higher **risk premium**.

The rationale for the choice of β, ε and δ parameters has remained largely unchanged since Case Study 1. The only difference is in the thresh-

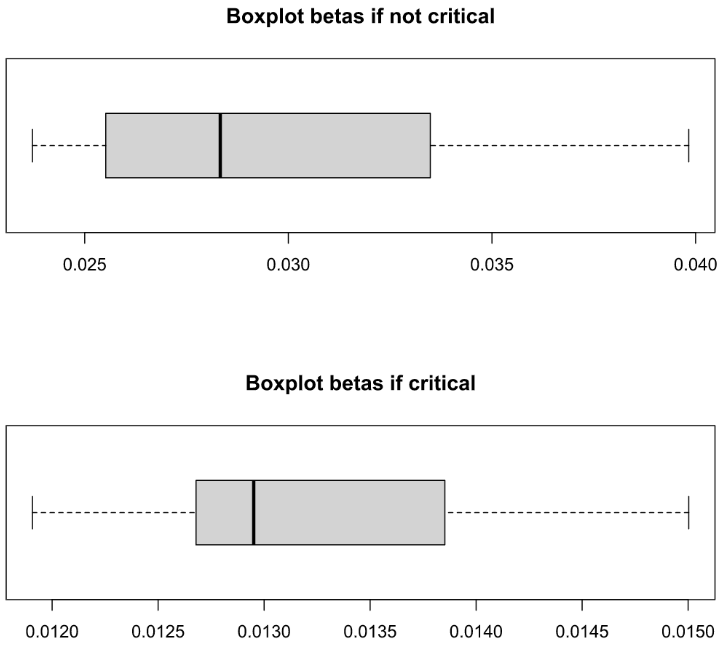


Figure 4.13: Case Study 2 - Betas boxplot

olds for beta. The new estimated betas are to vary between 0.04 and 0.02 and no longer between 0.03 and 0.01. As a result, the sigmoidal transformation expects betas such that the times to infection decrease. Consequently, all other things being equal, one expects an increase in the number of infections. In Figure 4.13 one can in fact see how the boxplots obtained from the matrix of betas reflect the desired characteristics.

Furthermore, you can see from Figure 4.14 how the times to infection were reduced in this Case Study 2. The mean of the distribution with the beta parameter (for non-critical and critical nodes) has been shifted substantially to the left. The algorithm used minimises the times to infection/recovery at each time instant, and consequently this leads to an advantage for infections. It should be noted, however, that varying the other parameters does not necessarily mean that this is the predominant behaviour, even if the beta value is increased. Indeed, one must consider the contribution of self-infection and the recovery process, which together can offset infections between nodes.

The Figure 4.15 summarises what has been said so far about the differ-

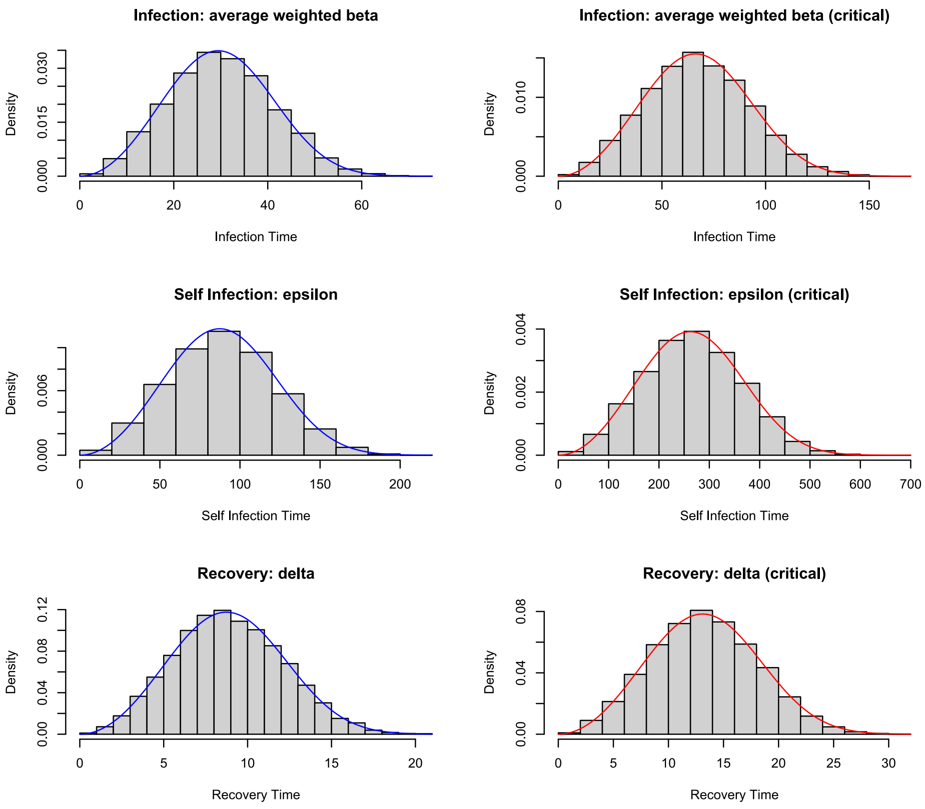


Figure 4.14: Case Study 2 - Beta, delta and epsilon distributions

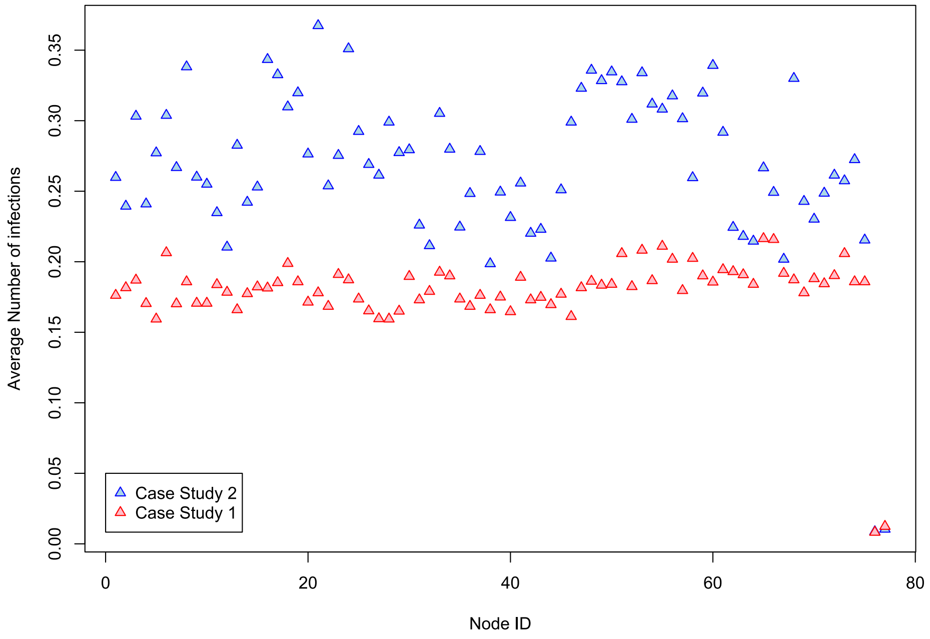


Figure 4.15: Average number of infections in Case Study 1 and 2

ences between CS1 and CS2. As can clearly be seen, CS2 leads to a higher average number of infections than CS1. It should be noted that this is not the case for critical nodes, as the number of connections between critical and non-critical nodes has remained unchanged. This is clearly a positive aspect as it means that, if well protected, critical infrastructures can be very resilient to cyber attacks.

As can also be seen from the equations, the risk premium in this case increases significantly (+17.40%). The same trend is also seen for the median and the 70*th* percentile of the distribution. The standard deviation, on the other hand, is smaller than in Case Study 1, probably due to the different (more homogeneous) topology of the network. A more connected network suggests less variability between nodes and thus less standard deviation, given the cost functions chosen for this analysis.

$$\mathbb{E}[\tilde{X}] = 8,483.05 \tag{4.7}$$

$$\mathbb{E}[\tilde{X}|\text{critical}] = 42,907.09 \tag{4.8}$$

$$\sigma(\tilde{X}) = 9,577.77 \tag{4.9}$$

$$\text{median}(\tilde{X}) = 7522.68 \tag{4.10}$$

$$p_{70\%}(\tilde{X}) = 8,375.36 \tag{4.11}$$

$$p_{99.5\%}(\tilde{X}) = 55,051.51 \tag{4.12}$$

As a final observation, it is worth mentioning that 20,000 simulations were carried out in both case studies, in order to try to capture as much of the tail behaviour of the distribution as possible (thus also considering the infections of critical nodes).

Conclusion

The purpose of this dissertation was to demonstrate that a cyber policy pricing mechanism for a small/medium-sized enterprise using a "micro" point of view is possible. This was demonstrated by simulating the network of interconnections between distinct nodes (devices) within the company and, using an epidemiological model, replicating infectious dynamics typical of hacker attacks e.g. *phishing*.

The positive aspects of this model are many and not trivial. By using a micro approach, it is possible to customise and tailor it to the individual company, shaping it to the needs of the insured and the insurer, setting *ad-hoc* (coverage) limits, and making it possible to study the dynamics and behaviour of the infection with an astonishing level of detail and granularity of information.

By using an epidemiological model of the $HG-SIS$ type, it was also possible to make use of a weighted network and thus to take into account the intensity of communication between different nodes. Furthermore, by introducing critical infrastructures, it was possible to have a qualitative distinction between nodes, since it is well known, even from a non-expert point of view, that it is difficult to put nodes into a single category. Nothing forbids extending the distinctions between nodes and generalising them into a set of distinct groups e.g. common nodes, managerial nodes, critical infrastructures, etc. By distinguishing node types, it was possible to introduce distinct distributions and cost functions, as well as distinctly different time-to-infection distributions for node types.

Furthermore, by introducing a function to generate networks with desired characteristics, it is possible to get an idea of what the final reward might be and to be able to make sensitivities. Ideally, it would be necessary to have a dataset of the company's internal communications (e.g. over the past year) and to reproduce the weighted graph, taking care also to consider the frequency of communications outside the graph. In reality, this information may not be available, at least not completely, and a function such as the one presented here makes it possible to get as close as possible to the "real" situation. It must also be kept in mind that, as this is not an easy and relatively risky business, the insurer may still want a more conservative approach, both in the amount of network connections and in the choice and calibration of the other necessary parameters.

The proposed approach also allows for extreme customisation in the choice of distributions. Some have been proposed such as the Weibull, Beta, truncated log normal, etc., but it goes without saying that they can be easily modified and calibrated to the individual entity to be insured and the characteristics of the policy. The biggest challenge is certainly the calibration of parameters such as those related to the distributions of times to infections. As for the recovery ones, they are somewhat simpler as they are highly dependent on the resilience of the company's IT department. Other parameters, such as those for times to infection and self-infection can be provided by expert-judgement or extrapolated from datasets and/or some real-time monitoring. It goes without saying that, using such an innovative approach, a conservative choice of these would be unavoidable.

In the event that it were necessary to use the proposed method with a large network (e.g. thousands of nodes), in that case some sort of clustering and 'trimming' of irrelevant nodes e.g. below a certain number of communications during the contractual term would be imperative.

There would certainly be an advantage from a computational and parameter calibration point of view.

The main challenges of this type of policy, however, remain rapid changes in the environment and types of attack that can disrupt the policyholder's and insurer's expectations. In this perspective, much remains to be done by cyber-resilience and regulators. What is certain is the *absolute need for reliable data* and information on these types of claims.

The motto that inspired the entire dissertation is the following:

Per ogni questione impiegare sempre lo strumento minimo che essa esige, minimo che è quasi sempre il massimo che essa comporta volendone trattare sul serio.

(For every issue, always employ the minimum instrument that it demands, a minimum that is almost always the maximum that it entails if you want to deal with it seriously).

B. de Finetti

Bibliography

[1] ANRA and Lloyds. "Il Rischio Cyber Fisico". In: *Upside Risk* 23 (2022). URL: https://cdn.anra.it/download/2119.

[2] The Geneva Association. *Insurability of Cyber Risk*. https://www.genevaassociation.org/publication/insurability-cyber-risk. Aug. 2014.

[3] C. Biener, M. Eling, and J. Wirfs. "Insurability of Cyber Risk: An Empirical Analysis". In: *Geneva Papers on Risk and Insurance - Issues and Practice* 40 (June 2014), pp. 1–28. DOI: 10.1057/gpp.2014.19.

[4] R. Böhme and G. Kataria. "Models and Measures for Correlation in Cyber-Insurance". In: *WEIS*. 2006.

[5] B. Bollobás. *Graph Theory*. ISSN. Elsevier Science, 1982. ISBN: 9780080871738.

[6] J.J. Cebula and L.R. Young. "A Taxonomy of Operational Cyber Security Risks. Technical Note CMU/SEI-2010-TN-028". In: (2010). URL: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9395.

[7] National Cyber Security Centre. *Cyber Essentials: Requirements for IT infrastructure*. 2022, p. 14. URL: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-0-January-2022.pdf.

[8] A. Charpentier. *Networks*. URL: https://github.com/freakonometrics/freakonometrics.github.io/blob/master/documents/teaching/LAUSANNE_2019_4.pdf.

[9] Clusit. *Rapporto Clusit 2022 sulla sicurezza ICT in Italia*. 2022.

[10] ENISA. *ENISA Threat Landscape*. 2021.

[11] ENISA. *ENISA Threat Landscape*. 2022.

[12] M.A. Fahrenwaldt, S. Weber, and K. Weske. "Pricing of cyber insurance contracts in a network model". In: *ASTIN Bulletin: The Journal of the IAA* 48.3 (2018), pp. 1175–1218. doi: 10.1017/asb.2018.23.

[13] World Economic Forum. "Global risks 2012". In: (2012). url: https://www.weforum.org/reports/global-risks-2012-seventh-edition.

[14] ISO/IEC. *ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary*. 2018.

[15] W.O. Kermack, A.G. McKendrick, and G.T. Walker. "A contribution to the mathematical theory of epidemics". In: *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character* 115.772 (1927), pp. 700–721. doi: 10.1098/rspa.1927.0118.

[16] A. et al. Kerstin. "Modeling and Pricing Cyber Insurance. A Survey". In: (2021). url: https://www.insurance.uni-hannover.de/fileadmin/house-of-insurance/Publications/2021/Modeling_and_Pricing_Cyber_Insurance.pdf.

[17] J. M. Lemnitzer. "Why cybersecurity insurance should be regulated and compulsory". In: *Journal of Cyber Policy* 6.2 (2021), pp. 118–136. doi: 10.1080/23738871.2021.1880609.

[18] M. et al. Malavasi. "Cyber risk frequency, severity and insurance viability". In: *Insurance: Mathematics and Economics* 106 (2022), pp. 90–114. issn: 0167-6687. doi: https://doi.org/10.1016/j.insmatheco.2022.05.003. url: https://www.sciencedirect.com/science/article/pii/S0167668722000610.

[19] H. et al. Märtens. "A time-dependent SIS-model for long-term computer worm evolution". In: *2016 IEEE Conference on Communications and Network Security (CNS)*. 2016, pp. 207–215. doi: 10.1109/CNS.2016.7860487.

[20] J. von Neumann. *Theory and Organization of Complicated Automata*. 1949.

[21] M. Nurek and R. Michalski. "Combining Machine Learning and Social Network Analysis to Reveal the Organizational Structures". In: *Applied Sciences* 10.5 (2020). ISSN: 2076-3417. DOI: 10.3390/app10051699. URL: https://www.mdpi.com/2076-3417/10/5/1699.

[22] OECD. *Enhancing the Role of Insurance in Cyber Risk Management*. 2017, p. 140. DOI: https://doi.org/https://doi.org/10.1787/9789264282148-en.

[23] M.S. Rahman. *Basic Graph Theory*. Undergraduate Topics in Computer Science. Springer International Publishing, 2017. ISBN: 9783319494753.

[24] Assicurazioni Generali S.P.A. *"Relazione sulla solvibilità e condizione finanziaria di Assicurazioni Generali S.P.A. 2021*.

[25] G. Strupczewski. "Defining cyber risk". In: *Safety Science* 135 (2021), p. 105143. ISSN: 0925-7535. DOI: https://doi.org/10.1016/j.ssci.2020.105143.

[26] P. Van Mieghem and E. Cator. "Epidemics in networks with nodal self-infection and the epidemic threshold". In: *Phys. Rev. E* 86 (1 July 2012), p. 016116. DOI: 10.1103/PhysRevE.86.016116.

[27] Verizon. *Data Breach Investigations Report*. 2022. URL: https://www.verizon.com/business/resources/reports/dbir/.

[28] X. Xie, C. Lee, and M. Eling. "Cyber insurance offering and performance: an analysis of the U.S. cyber insurance market". In: *The Geneva Papers on Risk and Insurance - Issues and Practice* 45 (June 2020). DOI: 10.1057/s41288-020-00176-5.

[29] M. Xu, G. Da, and S. Xu. "Cyber Epidemic Models with Dependences". In: *Internet Mathematics* 11.1 (2015), pp. 62–92. DOI: 10.1080/15427951.2014.902407. URL: https://doi.org/10.1080/15427951.2014.902407.

[30] M. Xu and L. Hua. "Cybersecurity Insurance: Modeling and Pricing". In: *North American Actuarial Journal* 23.2 (2019), pp. 220–249. DOI: 10.1080/10920277.2019.1566076.

[31] A. Yeftanus, S.W. Indratno, and R. Simanjuntak. "Cyber Insurance Ratemaking: A Graph Mining Approach". In: *Risks* 9.12 (2021). ISSN: 2227-9091. DOI: 10.3390/risks9120224. URL: https://www.mdpi.com/2227-9091/9/12/224.

Ringraziamenti

Vorrei ringraziare il mio Relatore per la passione verso le materie attuariali che ha trasmesso durante le sue lezioni. Quando mi sono immatricolato in questo corso di laurea sapevo a malapena la differenza tra un premio ed un sinistro. La mole di studio è stata impegnativa, ma, anche grazie ai suoi insegnamenti, rimango fermamente soddisfatto della preparazione ricevuta e degli standard accademici e professionali che sono stati trasmessi.

Un ringraziamento enorme va alla mia famiglia e ai parenti che non hanno mai smesso di supportarmi e di darmi coraggio.

Un grazie immenso a tutti gli amici che mi sono stati accanto e che hanno creduto in questa mia parte di viaggio. In particolar modo vorrei ringraziare Cristiana, Francesca, Meti, Guglielmo, Davide, Paolo e Lorenzo. Infine un ringraziamento particolare a Marco per il suo supporto instancabile, immancabile e mai cedevole.

Vorrei dire grazie anche alle persone che purtroppo se ne sono andate e non sono riuscite ad essere con me fino alla fine degli studi. So che sarebbero state contente per me e che, da qualche parte, sono lì a guardarmi.

Grazie a tutti.

Novara, 20/03/2023

Saverio Belvedere