Ca' Foscari
University
of Venice

amse
aix marseille
school of economics

Cyber risk in economics and finance

Master's thesis of:

Sonja-Lotta Jäämeri

matricola: 872118

Supervisor:

Roberto Casarin

Associate Professor of Econometrics

Ca' Foscari University of Venice

2018

Abstract

The 21st century is booming with the progress in technology and the expansion of artificial intelligence (AI). The fast development and adoption of Internet-based computer systems have left their users in misconception concerning the various risks associated with online networks. It is only recently that cyber risk has started to be seen as the serious threat that it is, which in turn reflects on the growing amount of research about the topic. In the aim of improving cybersecurity, the role of research is essential, as it raises awareness and contributes to a good breeding ground for cyber safety development. This thesis treats cyber risk through economic and financial aspects, and provides a review of the recent literature in the context of cyber risk. In particular, it discusses the part of cyber insurance in managing Internet risks, as well as the econometric frameworks introduced in previous studies to model cyber risk.

Contents

Introduction

Along with the expansion of information and communication technology (ICT) and the increasingly virtualised world, a new type of risk has been introduced to the modern society. Connected computer information networks, while an absolute necessity in the world of today, expose its users to a series of threats constituting cyber risk. Today's information society relies on the operation of networks and systems, which makes it highly vulnerable to interference. In fact, such systems face cyber attacks on a regular basis. Moreover, as many firms and organisations carry the same information technology (IT) infrastructure, they are object to correlated risks. This introduces further challenges to managing cyber risk, since it makes the threat spread and grow very fast. Furthermore, throughout the few past decades, cyber attacks have developed to be more sophisticated and widespread causing disruption to public services, business and administration, and hence to the functioning of the society as a whole.

In response to this evolution, cybersecurity and cyber risk management have become an important topic in boardrooms as well as a central point in the political agenda of countries that are strongly dependent on information systems. They are considered to be an essential part of the society's overall security. In fact, on September 13, 2017 The European Union published some fresh guidelines[1] for strengthening cybersecurity in the EU. In terms of the goal of creating a powerful "digital Europe", cybersecurity is defined as a necessity for the pursuit of global digital leadership. This is because, if carried out, cyber risk is a security threat, which jeopardizes the correct or intended function of the targeted information system. At worst, it can disturb and even paralyze some components of the societies' critical infrastructures and vital functions. Electricity and energy distribution, water filtering plants, healthcare services, phone data and food transportation all lie upon numerical Internet-based systems subject to perturbation. Thus, not only is it crucial to identify the vulnerabilities and employ according protection but also to develop new, and further improve existing, cyber security strategies.

[1] "Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", European Commission, September 13, 2017

The aim of this thesis is to analyse cyber insurance, investigate some existing tools to model cyber risk and discuss their importance from an economic and financial perspective. The structure of the remainder of the research is organised as follows. Chapter 1 is a review of the recent literature on cyber insurance, chapter 2 treats the modelling frameworks developed in econometrics to measure, model and predict cyber risk, and chapter 3 is an overview of the current state of the cyber insurance market.

1. Economics of cyber insurance

Cyber risk is indeed a rapidly evolving threat, which requires the imperative attention of specialists from all domains. The different alternatives for managing cyber risk and the heterogeneous behaviour of fellow users on the Internet make it harder to identify the breadth of the threats. It can therefore be difficult to establish the appropriate amount of resources to dedicate to cyber security. Thus, cyber risk management provides a key for two critical problems. It allows to reduce the exposure of network systems to the risk and it enables entities to determine the optimal distribution for their security investments.

After acknowledging the problem, the range of ways to manage cyber risk is not endless and can basically be restricted to four different options [45], [11]. First, one can try to avoid the risk, which however seems somewhat utopian in the IT dominated world of today. Another option simply consists in keeping the risk and accepting the losses whenever they take place, which in the long term, however, could end up being very costly. The third one is to self-protect and mitigate the risk, which in turn requires some personal or internal investments, such as time or money, as it means that an entity protects its infrastructure on its own. Besides, regardless of whether the entity protects itself well or not, it can only minimize the probability and magnitude of the losses but can never eliminate the risk entirely. Finally, an entity may decide to transfer the risk or part of it to someone willing in the form of a contract or hedging. This is, for example, the case of cyber insurance. The two parties, the insurer and the one seeking to be insured, can agree on some terms and form an insurance contract, by which the risk is removed from the insured and transmitted to the insurer in return for a certain amount of money, i.e. a premium payment.

The first objective of this analysis is to review the context of cyber insurance as a cyber risk management tool. This chapter addresses the plausible incentives for insurance companies to provide cyber insurance as well as the layout of the challenges related to insuring cyber risks. It also introduces a basic modelling framework for the risk along with the procedure by which insurers construct policies to cover modern and complex risks.

1.1. Motivation for insurers

1.1.1. Seizing the market opportunity

Cyber risk management has without a doubt become a key element of the modern society. As important technologies and infrastructures began to digitalize, malicious actors became interested in the increasing amount of delicate information stored online, since is accessible from anywhere around the world hence making it possible for them to act without geographical restraints. Fortunately for insurers, where there is a problem, there is an opportunity. In fact, the progressive range of cyber attacks has created a powerful business opening for insurance companies and other independent insurers allowing them not only to develop new products and policies but to serve organisations in need for assistance.

The growing attention towards matters related to cybersecurity have started to show in companies' attitudes and risk management. While the risk itself is enough, the way it is managed and the implemented security proceedings in case the risk materializes contitute an additional risk to the companies. Consequently, boardrooms have began addressing the issues regarding cyber risk management in a more serious tone and perceiving cybersecurity as an inevitable part of companies' investment strategies. As the number of attacks continues rising, companies build stronger defence structures to predict, detect and report these attacks. At the same time, however, regulations are changing and the spectrum of attacks is becoming more versatile and elaborate, which makes it challenging and time-consuming for companies alone to keep up with. Therefore, insurers have a critical role in contributing to the stability of the activity of businesses and other organisations.

1.1.2. Competitiveness

It is logical that the supply of cyber coverage grows with the development of finer technology and data tools. In addition to cyber specific insurers, an increasing amount of traditional insurance service providers offer cyber risk coverage. The insurance industry is a competitive field and insurers struggle to stand out and differentiate themselves from their rivals. Product availability may be a threshold issue for certain insurance customers, and for reasons of possible package deals and practicality, entities often tend to acquire all the necessary insurance from a single insurer. In this way, the absence of cyber coverage supply could lead to entities choosing to go with another insurance company not only for a cyber insurance policy but for their other policies as well. Although the cyber insurance market is far from reaching its full potential, several insurance companies on the market offer coverage against cyber threats. Furthermore, the fact that insurers themselves carry potentially a great number of policies and a lot of sensitive client information justifies the emergence of a reinsurance industry. Chapter 3 provides a more detailed discussion of the cyber insurance market and its actors.

1.1.3. Improving overall Internet security

By providing cyber insurance coverage, insurers can improve the general level of security on the Internet. That is to say, not only the risk of the insured is reduced but also that of other network users. As more cyber insurance is sold there is an increase in cyber security investments, which in turn translates into a safer network. This results in the insured's probability of experiencing a cyber attack being below its previous level implying a lower expected loss for the insurer. Moreover, cyber insurance creates an important incentive for entities to invest in self-protection [11], which then has a positive effect on the state of the network. Thus, the supply of cyber insurance promotes the overall security on the Internet, while simultaneously generating more stability into the insurers' own activity.

1.1.4. Nascent legislation

Regulation is a big factor in affecting the market for cyber insurance. Indeed, the demand for cyber coverage depends on political decisions and effective laws (e.g. data privacy). To site some of the most significant influencers, May, 2017, the White House published an executive order in the aim of stregthening cybersecurity of critical infrastructures[2]. February, 2018, the Securities and Exchange Commission (SEC) released updated guidance on cybersecurity[3]. Finally, the fresh entry into force of the General Data Protection Regulation 2016/679 (GDPR)[4] in May 2018 is likely to further boost the market. In fact, as the regulatory framework expands, the major financial and private information holders, such as industrial leaders, banks and other service providers, including insurance companies, require up to date security mechanisms and risk management support systems. This in turn creates an opportunity for both the cyber insurance and the cyber reinsurance market.

1.2. Challenges of cyber insurance

1.2.1. Rapid evolution of risks

Cyber risk is a fast-growing threat and it is therefore hard for insurance companies to keep up with developing policies to cover it. Besides, in cyberspace the threats are not limited by physical constraints such as distance or location. A cyber attack can affect far from where it is originated,

[2] Please see: "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", Infrastructure and Technology, May 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[3] Please see: Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures", February 21, 2018, 17 CFR 229, 249, [Release Nos 33-10459; 34-82746], https://www.sec.gov/rules/interp/2018/33-10459.pdf

[4] Please see: European Commission, "Communication from the Commission to the European Parliament and the Council, Stronger protection, new opportunities – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018", January 1, 2018, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf

and it can reach the opposite side of the world almost instantly. In contrast to "real life" criminals, the creators of an Internet malware do not have to worry that much about eyewitnesses or leaving behind concrete evidence, since often by the time the invasion is detected the attacker has already had the time to cover all possible traces. Cyber attackers do not use their own computers but instead they typically take control of somebody else's network system, or many systems, and use them to implement the malicious activity. Furthermore, they apply encryption procedures, which can turn out unbreakable for security agencies. This makes cyber criminals extremely difficult to track down. In addition, there tends to be a significant lack of understanding on the risks of the Internet among its users. This, in turn, affects the state of the network making it more ambiguous and less predictable for the insurers.

As the occurrence of cyber threats is random, it is difficult for insurers to predict the losses. In addition, the supply of cyber reinsurance is lacking, which makes it further challenging for cyber insurers to cover their risky policies. Moreover, risk sharing among insurance companies is not effective due to the small size of the risk pools and the lack of exposure data. Although, as more and more insurance companies enter the market, the risk pools become larger and this problem is reduced [9].

1.2.2. Correlation among risks

A correlated risk consists of the situation where one single event brings on a simultaneous occurrence of multiple losses. This type of risk is often associated with natural disasters because of their tendency to cause disruption on a large scale. The influence on the distribution of losses is such that, for a same level of expected loss, correlated risks have a higher variance than independent ones [65]. In finance and insurance theory, a higher variance is associated with a higher level of risk. This is because, the square-root of variance is the standard deviation, which is a measure of volatility from the mean, and volatility itself is a measure of risk. Hence, variance is also a measure of risk. Moreover, a greater deviation from the mean translates into more risk, and thus the conclusion that a larger variance indicates a higher risk. In fact, given that the variance of correlated risks is higher than that of uncorrelated ones, the former contain a bigger risk.

For example, assume an insurer sells two insurance policies against a risk with the probability of a loss $p = 0.2$ and the size of the loss $L = 1000€$. If the losses are uncorrelated, the probability that there are two losses is: $0.2×0.2 = 0.04$, which corresponds to the loss: $0.04×2×1000€ = 80€$. In this case, the probability of one loss is: $0.8×0.2 + 0.2×0.8 = 0.32$, leading to an expected loss of $0.32×1000€ = 320€$. The chance that there are no losses is: $0.8×0.8 = 0.64$. If the losses are perfectly correlated with each other, then there can either be two losses or no losses at all. In these circumstances, the probability of two losses is simply 0.2, with an expected loss of: $0.2×2×1000€ = 400€$, and that of no losses is 0.8. As can be seen, whenever there is at least one loss, the consequences in the second case are more severe [65].

Let us generalize the previous example to the case, where n is the number of insurance policies, m is the number of losses, p is the probability of a loss and L is the size of a loss. If all of the policies are perfectly correlated, then there could either be no losses, in which case the loss is equal to 0€, or there could be $m = n$ losses, which in turn corresponds to a loss of $p \times n \times L$ € (with $m = n$). However, if the policies are independent, we have the following loss:

$$\{\ p^m \times (1-p)^{n-m} \times \binom{n}{m} \times m \times L\,, \qquad p \in [0,1]\,, \qquad m \in [0,n]\,, \qquad n \in \mathbb{N}^+\,, \qquad L \in \mathbb{R}^+ \,\},$$

where:

- p^m is the probability of m losses
- $(1-p)^{n-m}$ is the probability of the remaining $(n-m)$ non-affected policies
- $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ corresponds to all the possibles scenarios of m-combination of losses from a set of n insurance policies
- $m \times L$ is the total amount of loss generated by the m losses.

By simply comparing the two, it is easy to see that the expected loss from correlated policies is more substantial than the loss caused by independent policies:

$$(1) \quad p^m \times (1-p)^{n-m} \times \binom{n}{m} \times m \times L \leq p \times n \times L$$

Substituting $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ in the expression above yields to:

$$(2) \quad p^m \times (1-p)^{n-m} \times \frac{n!}{m!\,(n-m)!} \times m \times L \leq p \times n \times L$$

In order to simplify the comparison, the terms can be rearranged, and $p \times n \times L$ can be isolated on the left-hand side of the inequality, which gives:

$$(3) \quad p^{m-1} \times (1-p)^{n-m} \times \frac{(n-1)!}{(m-1)!\,(n-m)!} \times p \times n \times L \leq p \times n \times L$$

Finally, all there is left to prove is that the following resulting outcome holds:

$$(4) \quad p^{m-1} \times (1-p)^{n-m} \times \frac{(n-1)!}{(m-1)!\,(n-m)!} \leq 1.$$

That is, to verify whether it is true, we need to study the limit of the expression on the left-hand side of the inequality. The limit can be defined by observing only the term with the highest degree, i.e.:

$$(5) \quad \lim p^{m-1} \times (1-p)^{n-m} \times \frac{(n-1)!}{(m-1)!\,(n-m)!} = \lim p^{m-1} \times (1-p)^{n-m}$$

Since p and $(1-p) \in [0,1]$, we know that $p^{m-1} \times (1-p)^{n-m} \in [0,1]$ with $m \leq n$. This means that inequalities (1) to (4) indeed hold, and consequently the expected loss that results from correlated risks exceeds that from uncorrelated risks.

Due to the important variance, a high level of correlation among insurance policies increases the probability of extreme losses, which in turn complicates the pricing of premiums for insurers, and makes them add more safety loadings to the pure premiums, i.e. charge greater premiums to their clients. In fact, whenever policies are correlated it is not enough for risk adverse insurers to cover their expected losses, as they also need to protect themselves against the greater probability of disasterous losses induced by the correlation [65].

The correlation of risks has been recognized as a problem and studied in the framework of cyber insurance on several occasions, (e.g. [14], [16], [69], [38], [51], [11], [31]). Öğüt, et al. [69] and Bolot and Lelarge [11] analysed the implications of correlated risks on public policies and self-protection and found that in the presence of correlated risks firms do not invest enough in self-protection and insurance relative to the social optimal levels. Another relevant conclusion in [69] is that the degree of risk correlation increases with the number of firms.

Böhme and Kataria [14] did an extensive research on modeling and measuring the correlation of risks in cyber insurance and provide a two-tier approach to the categorization of the different correlation properties associated with cyber risks. They take into account both the global correlation between independent entities (firms) and the correlation among cyber risks within the internal network of a firm. They found that while cyber insurance is a good option for entities with high internal correlation it does not work very well with high global correlation. In fact, high global correlation leads to inaccurate estimations by the insurers, increasing the probability that their losses exceed the amount they anticipated for the period. This drives them to load the premiums, which then further confines the supply of cyber insurance. Entities with low internal correlation, on the other hand, are able to manage the risk and self-protect their own network system. Therefore, they may not need to transfer the risk. Thus, the classes of risk with high internal and low global correlation are best adapted for cyber insurance [14].

1.2.3. Interdependence of risks

Another feature of cyber risks is that they are interdependent. This means that while the risk of an entity is obviously related to its own security enforcements, it is also affected by that of others. In other terms, how cyber risk is managed by any entity, and the investments they make to promote their security, influence the overall risk on the Internet.

According to Kunreuther and Heal [41] and Öğüt, et al. [69], the incentive for security investments and insurance coverage decreases with the interdependence of risks. This is because the fact that whether investing in security is profitable or not is contingent on the security efforts enganged by others. Due to this interconnection, although an entity invests in a defense system against the threat itself, it is also put in jeopardy if other computers on the network have insufficient protection. For example, assume two collaborating companies, one of which has invested in security (A) and the other not (B). If a malware occurs and B is touched, given the tight professional relationship between A and B the malware can easily spread into A's IT system through what would be perceived as safe business communication with B. That is to say, despite its own security investments, A would be confronted with a high risk of infection.

This interdependence generates externalities, when entities allocate their security resources inefficiently. In fact, the externalities are positive or negative depending on whether they under- or overinvest in cyber security. Shim [58] analysed cyber risk management from the point of view of interdependent security risks and demonstrated the impact of different types of cyber attacks on externalities. His study supports the idea that the interdependence of IT risks creates externalities. Moreover, it shows that in presence of interdependent risks the firms' investments in security cause positive externalities whenever they are made to cover untargeted attacks (e.g. worms, viruses, systemic risks) and negative externalities when made to cover targeted attacks (e.g. security hacks, spear phishing, waterholing, malicious USB keys). Therefore, the positive externalities in the case of untargeted intrusions correspond to entities allocating deficient resources in security (underinvestment), whereas the negative externalities in the case of targeted intrusions mean entities overinvest in cyber security.

As for insurers, the risk associated with untargeted attacks is greater than the one associated with targeted attacks because of the underinvestment [58]. Consequently, insurance companies have to set the premium prices in such a way that they cover the additional losses arising from these targetless attacks. If they would simply charge higher premiums for the coverage against untargeted attacks, people would be discouraged to invest in security and purchase insurance for these types of attacks, which in turn would further exacerbate the problem of underinvestment. Indeed, while many would be demoralized by the expensive premiums, the entities who would decide to insure themselves would end up paying more for their coverage just to be compromised by the unprotected. Furthermore, the insurance price against targeted attacks being lower in that case, the entities are drawn to cover them instead, which on the other hand contributes to the overinvestment issue. In fact, insurers should set a lower price for the untargeted attacks than the targeted ones, since it would drive entities to buy coverage for the former and reduce the exessive investments related to the latter [58]. Zhao, et al. [67] suggest that, when applied on several firms, managed security services, such as firewalls and antivirus services, are better at mitigating the inefficient investment problem, as their providers are able to explicitly take into account all network externalities before deciding on the security investment strategies.

1.2.4. Asymmetry of information

In economics and finance, whenever there is symmetric information between the parties of a contract, the market is efficient, whatever the market power. However, when this information is asymmetric, one of the parties holds private information, i.e. some information that is relevant for the implementation of the contract but limited only to his/her knowledge. The information asymmetry generates a disproportion of power between the two parties, since there is no way for the other party to get hold of the private information. The problem and the way it is managed can lead to the failure of the market.

The asymmetry of information has throughout time had an important role in insurance. By one, insurance markets are characterized by adverse selection and secondly they are affected by problems associated with moral hazard. In economics, the issue of adverse selection is often illustrated by the example in Akerlof's (1970) famous paper "The Market for Lemons" [4], in which Akerlof applies the problem of quality uncertainty to a second-hand car market. He concludes that, given the information asymmetry between sellers and buyers on the market and, as both cars sell at the same price, the buyers' inability to identify whether they are dealing with a "good" or "bad" seller, the sellers of "good" cars withdraw themselves from the market leaving only "bad" cars ("lemons") on the market. More generally, adverse selection is a situation, where due to asymmetrical information, the parties with private information benefit from contracts on the account of the other parties with inferior knowledge. In cyber insurance, adverse selection occurs when insurers have an incomplete perception of the vulnerability of their potential clients as they are uncapable of distinguishing between high and low risk ones prior to signing the contracts. The problem manifests itself once the insurers' lacking knowledge on the exposures and the absence of price discrimination lead eventually to the high risk clients purchasing more insurance than the low risk clients. At worst, it can lead to the low risk clients disappearing and the market collapsing.

Along with adverse selection moral hazard is a well recognised problem in the insurance industry. However, unlike adverse selection, moral hazard refers to a change in one of the parties behaviour on the detriment of the other party after the contract has been signed. In insurance, it typically corresponds to the insured party becoming more negligent or engaging in unnecessarily dangerous activity as soon as the insurance comes into effect. Consequently, the insurer is ultimately unaware of the actual amplitude of the risk associated to the policy in question and ends up underestimating the probability of loss. Although there exist some support for these types of situations, it is difficult for insurers to control their clients behaviour during the entire term of contracts as they often have many clients and dispose of limited resources to keep track of all of them.

As for cyber insurance, moral hazard is particularly troublesome in the context of third party liability. Policy provisions allow insurers to define some ground rules and assign some responsibility to the insured but are insufficient whenever the insurer is liable to a third party [6]. For example, the case where due to its lack of self-protection, an insured bank undergoes a data breach resulting to the disclosure of sensitive client information. While the insurer (second party) can dispute the indemnity payment for the bank (first party) under policy provisions regarding appropriate self-protection, it may still be liable to the clients of the bank (third party), who have themselves suffered losses because of the exposure. Furthermore, according to [6], the insurance compensation for these types of liabilities encourages the insured to invest the minimum in security in order to obtain coverage and to clear further responsibility with regards to its clients by purchasing insurance. This increases the risk held by the insurer as well as the damages endured by the clients. On the one hand, the adoption of deductibles allows insurance companies to share some of the financial burden with the insured. On the other hand, they penalize policy holders for making the security investment and thus lower their motivation to purchase coverage. Consequently, more efficient ways to steer the the insured into responsible behaviour include premium discrimination per unit of risk exposure (risk rating) and the choice of insurable risks (underwriting) [6], [3].

As was noted by Agrawal and Shivendu [3] in their study on cyber insurance, the empirical study on the impact in the cyber insurance industry of asymmetrical information, namely adverse selection and moral hazard, is not conclusive. This can be due to the fact that, while the issues arising from information asymmetries can lead to catastrophic consequences, they have already long been a well established nuisance in all insurance markets. In fact, the problems of adverse selection and moral hazard, as we perceive them now, have actively been adressed in the economic literature in the aim of improving the functioning of markets ever since around the 1960s. For this reason, insurers have developed a better understanding of the problem and learned to mitigate it.

1.3. Cyber insurance modelling

The modeling of IT insurance is not that far from traditional insurance models. Like other branches of insurance, cyber insurance is shadowed by the issues of information asymmetries. The main difference is in the nature of the risk. As discussed above, cyber risks are correlated and interdependent, which needs to be taken into account when defining the model. In recent literature, cyber insurance has often been modeled from the perspective of expected utility and asymmetrical information (e.g. [28], [11], [69], [46]) or by means of copula functions (e.g. [15], [16], [51], [31], [66]).

The main motivation for applying copula functions is that they take into account the dependence between variables that do not follow the same distribution [31], [66]. They separate the dependence structure and the univariate marginals, which in turn enables the modeling of any type of distribution function. The separation is possible using the result of Sklar's theorem (1959)[5], according to which it is possible to express multivariate cumulative distribution functions (cdf) in terms of copulas. It allows to express an n -dimensional joint distribution function F of n random variables $X_1, \dots, X_n$ with respective marginal distribution functions $(F_1(X_1), \dots, F_n(X_n))$ in terms of a copula $C(F_1(X_1), \dots, F_n(X_n))$. Thus, this corresponds to: $F(X_1, \dots, X_n) = C(F_1(X_1), \dots, F_n(X_n))$. The theorem is reversible in the sense that for any $F_1(X_1), \dots, F_n(X_n)$ of distribution functions and any copula C, the function F is a n -dimensional distribution with marginals $F_1(X_1), \dots, F_n(X_n)$. In addition, C is unique whenever $F_1(X_1), \dots, F_n(X_n)$ are continuous. This is useful since, while the margins $F_1(X_1), \dots, F_n(X_n)$ can usually be found quite easily, their joint distribution F may be

[5] For the proof of the theorem please see Sklar (1959) and Schweizer & Sklar (1974)

difficult to identify. Therefore this theorem demonstrates the important role that copulas have in empirical research. Furthermore, copulas are useful in modeling nonlinear relations, which occur as marginal distributions are not normal [31], [66], [14]. For these reasons, they are well suited for the specification of cyber insurers' loss functions.

Herath and Herath [31] use ICSA data and consider the number of computers affected by a malware to represent the magnitude of the threat and provide a framework for modeling cyber risk in the context of first party damage insurance using a copula-based methodology.

1.3.1. Loss function for cyber risk

Loss functions are used in insurance to represent the actual amount of indemnities paid to the policy holders after having taken into account payments by the insured, such as deductibles and premiums. Relying on the work done in [31] for the copula modeling of the loss distribution, the following framework may be considered, where:

- R is the sum of money reimbursed in the event by the insurer to the insured
- ℓ is the amount of the loss, which is the joint loss distribution associated with the number of affected systems a and the losses observable from the data θ,

the loss can be defined as $\ell = h(\theta, a)$.

The loss distribution function can be defined using an interval into which the total number of affected systems a most probably falls: $[a_{min}, a_{max}]$. Simulating the amount of loss by the number of systems affected ($\ell = h(\theta, a)$) and setting k_i as constants leads to the following loss distribution function for a given policy holder:

$$\ell = \begin{cases} k_1, & \forall\ a \in [0, a_{min}[\\ k_2 + \left(\frac{a - a_{min}}{a}\right)\left(\frac{\theta}{10}\right), & \forall\ a \in [a_{min}, a_{max}[\\ k_3 + \left(\frac{a - a_{max}}{a}\right)\left(\frac{\theta}{10}\right), & \forall\ a \in [a_{max}, +\infty[\end{cases}$$

The values of $\ell = h(\theta, a)$ can then be obtained by sampling on a Monte Carlo simulation method [31], which is appropriate for modeling several variables simultaneously. Monte Carlo simulations essentially consist of three stages [19], which are repeated through multiple iterations:

1. Selection of probability distributions according to which arbitrary values are assigned to each random variable
2. Execution of the underlying model with the values from step 1
3. Collection of the results obtained in step 2

1.3.2. A probabilistic copula model for cyber risk premium

In the case where there are no deductibles or limitations in the policy, the reimbursement is simply the loss function and we have: $R = \ell = h(a, \theta)$. However, the insurer and insured may agree on some additional features relevant to the contract to reduce the insurer's liability. Typically, these include the possibility of deductibles and coinsurance as well as defining a limit up to which extent the indemnification can go. In this framework, as represented by [31] the reimbursement by the insurer is the following:

$$R = \begin{cases} 0, & \forall\, \ell \in [0, d] \\ (1-c)(\ell - d), & \forall\, \ell \in \left]d, d + \dfrac{l}{1-c}\right[\\ l, & \forall\, \ell \in \left[d + \dfrac{l}{1-c}, \infty\right[\end{cases},$$

where:

- d is a deductible at the expense of the policy holder
- c is the percentage covered by the policy holder in coinsurance
- l is the limit of the indemnification, i.e. the threshold over which the exceeding losses are not covered by the insurer

Whenever the loss is lower than the amount of the deductible (d) the reimbursement by the insurer is equal to zero, since d is paid by the insured party. If the loss (ℓ) is beyond d, the insurer pays $1 -$

c percent of the exceeding loss $(\ell - d)$ until ℓ reaches the point from where the compensation is a constant and equal to the limit (l).

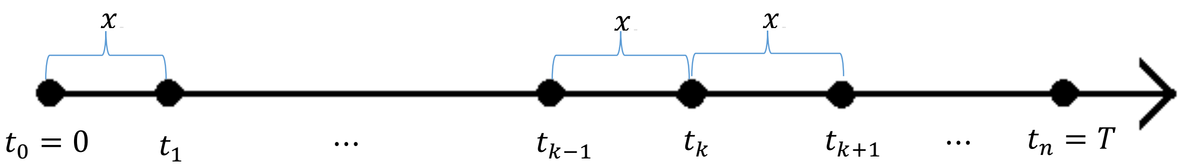
Assuming that there cannot be more than one claim made by the policy holder per period, the model for the insurance premium (net from profits and expenses) can be computed as the following expected value [31]:

$$E(P) = E(\eta e^{-\delta t} R) = \bar{\eta} E(e^{-\delta t}) E(R)$$

where:

- P is the net cyber insurance premium price
- $\eta \in \{0,1\}$ is a dichotomous variable, which takes the value 1 in case of a claim and 0 otherwise
- δ is known and corresponds to a discount rate
- $t \in \mathbb{R}_+$ is an unknown variable that represents the time between the signing of the contract and the payment of the indemnification to the policy holder. t can be estimated by considering that the compensation is paid at the same time as the threat materializes. Although in reality this is rarely the case, it provides a simplification without much loss of generality.
- $\bar{\eta}$ is the expected value of η, i.e. $E(\eta) = \bar{\eta}$ or equivalently the probability that η takes the value 1, i.e. $proba(\eta = 1)$. For simplicity, $\bar{\eta}$ is assumed to be equal to one whenever there is a loss, i.e. $\ell > 0$.

A Poisson model is used in [31] to obtain a proxy value of the unknown t. Poisson distributions are widely used in finance and insurance as they allow the modeling of abrupt events that may occur at any instant of time. The mathematical foundation behind the model can be illustrated with the following timeline:



As can be seen above, the interval $[0, T]$ is divided into n equally spaced points, and $t_i \in [t_0, t_n]$. The distance between each t_i is $\frac{T}{n} = x$ and as $x \to 0, n \to \infty$. By following the steps in [31], t can be estimated by simulating a Poisson process. The methodology consists in applying the following process:

$$t_i = t_{i-1} - \left(\frac{1}{\lambda}\right) \ln u$$

where:

- λ is the expected number of cyber attacks per unit of time
- $t_1 - t_{i-1}$ are independent exponential random variables with a mean equal to $\frac{1}{\lambda}$. They represent the difference in time between any pair of consecutive cyber attacks given that $t_0 = 0$.
- $u \sim U(0,1)$ is a uniformly distributed random variable, uncorrelated with the other variables in the model

The simulation is done by first drawing the input $u \sim U(0,1)$ and substituting it in the expression above, which in turn can then be executed and returned to ultimately collect the outcome.

Finally, the copula model for cyber insurance premium pricing can be estimated by creating an algorithm with the steps provided in [31]. The simulation procedure is the following:

1. Determination of a copula to fit in the data (θ, a)
2. Simulation of bivariate outcomes (θ_j, a_j) for iteration j with the copula defined in step 1
3. Computation of $\ell^j = h(\theta_j, a_j)$ for each (θ_j, a_j)
4. Simulation of the Poisson process described above to extract t^j
5. Computation of $P = \eta R e^{-\delta t}$ for iteration j, i.e. $P^j = \eta R^j e^{-\delta t^j}$
6. Computation of $E[P]$ and $\sigma[P]$ with N the total number of iterations:

$$E[P] = \frac{1}{N}\sum_{j=1}^{N} P^j$$

$$\sigma[P] = \sqrt{\frac{\frac{1}{N}\sum_{j=1}^{N}(P^j)^2 - [E[P]]^2}{N}}.$$

The copula model is for first party cyber insurance, and can be applied on policies with or without additional features. The actuarial approach relies on data about the number of affected computers, which can be found in the ICSA survey (2003). However, the estimation could be improved by loosening on the assumptions. For instance, a more precise approximation for η could lead to better results [31]. Furthermore, more recently, new databases have been created to collect data on losses (e.g. NetDiligence (2014), SAS OpRisk Global Data (2015)) [21], which could be used to obtain even more accurate estimates.

As technologies are constantly evolving and the cyber risk landscape is changing, the correct perception of risks and the appropriate specification of the premium are very important in cyber insurance, and might even form the determinant survival factor for insurance companies. The next chapter contains a more comprehensive review of the different insights in measuring and modeling Internet risks.

2. Econometrics of cyber risk

The second objective of this thesis is to inspect the econometric methods used to measure, model and predict cyber risk. The relatively young age of IT, the amount of literature available on cyber risk, and the increased involvement of different economic and political institutions in the matter suggest that we are dealing with a very serious and extensive risk. However, similarly to any kind of risk, cyber risk is just as great as the vulnerability behind it. Therefore, all entities, such as individuals, organisations as well as governments, relying on Internet-based computer systems, need to determine their potential risk factors to be able to take action accordingly. From there, the assessment of cyber risks follows a certain pattern. The first step is to identify the infrastructures involving cyber risk and gather information on the exposures. This is followed by an analysis on the feasible cyber threats and an estimation on the frequency of their occurrence. Finally, risk management decisions, such as the allocation of security resources, are made basing on the data from the model. The complicated part of the cyber environment is that it changes so fast and unsuspectably, meaning that the models need to be revised and readjusted regularly. That is to say, cyber risk assesment is a continuous process, which relies on available information about threats and on the advances in the development of methods to manage these threats, thus highlighting the important role of research on cyber risk. This chapter treats some basic mathematical and statistical modelling frameworks applied in econometrics to mitigate cyber risk.

2.1. Measuring cyber risk

2.1.1. Cyber risk perceptions and preventive measures

In order to fully grasp all the dimensions of cyber risk and to develop accurate and effective protection against it, we must understand how it is perceived by people and what actions, if any, they take to respond to it. The concept of risk perception is frequent in economics and finance, namely in utility theory, and is often referred to as an agent's attitude towards risk. Utility and indifference curves[6] are broadly used in the supply and demand analysis to model the functioning of goods markets, as well as in social welfare economics to analyse Pareto efficiency. In finance, utility is applied in risk measurement and to generate indifference prices, i.e. subjective prices for given assets. Therefore, the utility function must have such properties that it takes into account the agent's risk aversion.

More precisely, in expected utility theory, the agent's attitude towards risk is represented by the shape of the curve of the utility function. That is, whenever the utility function $u(\cdot)$[7] of the agent is

[6] An indifference curve is the plot of the combination of consumable goods or services that would allow one to maintain a given level of satisfaction (see Edgeworth's box, Mathematical Psychics: An Essay on the Application of Mathematics to the Moral Sciences, 1881)

[7] Please see expected utility, the von Neumann-Morgenstern utility theorem (1944) and risk aversion

convex, i.e. $u(\overline{w}) \leq E[u(w)]$ (w being a random variable with mean $\overline{w}$) the agent is considered to be "risk loving", whereas a concave utility function, i.e. $u(\overline{w}) \geq E[u(w)]$, corresponds to a risk adverse agent. The utility function of risk neutral individuals is linear $(u(\overline{w}) = E[u(w)])$. Furthermore, since these properties hold, $u(\cdot)$ is invariant under any positive affine transformation. In other terms, the classification remains unchanged, when the designated utilities are subject to a positive affine transformation. In practice, this means that $v(w) = au(w) + b$ and $u(w)$ correspond to the same attitude towards risk from the agent. However, the utilities need to be normalised (e.g. $u_{min} = 0 \ and \ u_{max} = 1$, $u_{min} \ and \ u_{max}$ being the lowest (worst outcome for the agent) and highest (best outcome for the agent) values of utility). The financial agent is generally assumed rational, which translates into risk adverse.

Internet users' attitudes towards online risks and their effects on preventive behaviour have attracted many reasearchers' interest in the past few years (e.g. [33], [34], [25], [26], [63]). Van Schaik, et al. [63] apply statistical methods to study US and UK students' risk perceptions regarding different cyber risks as well as the security measures undertaken by them to mitigate the risk. To provide information about how cyber risk is perceived among the students, they consider a categorized list of Internet functions and associate them to a set of cyber risk features. The analysis shows interesting findings concerning the participants' attitudes towards IT security risks and the protection they have:

1. US and UK students' risk perceptions do not differ much from each other. More or less the same online activities are perceived as riskiest and least risky by the two groups of students.
2. The top five attacks viewed as most serious are identity theft, keylogger, cyber-bullying, social engineering and virus attacks with the highest mean values for perceived risk, whereas online browsing, cookies and email harvesting were seen as least risky.
3. While the general level of self-protection is high among both US and UK students, the participants tend to rather rely on anti-virus software or operation and security system updates as opposed to the less familiar anti-spyware and firewall add-ons.

Research on how well the risks of the Internet are understood and managed by its users facilitates the identification of vulnerabilities, and hence, the dissemination of awareness concerning cyber risk, as well as the development of efficient protection systems and policies to cover the risks. Although past studies provide a somewhat common and thorough view of cyber safety behaviour, it is worth mentioning that the analysis is predominantly concentrated on the security measures employed in nonportable devices. However, an increasing number of Internet applications are accessed from portable devices. For instance, money transfers, payments and other bank services are available on mobile phones. In addition, a considerable amount of private and work related information is communicated through portable devices, making them exposed to a high level of risk. According to Bank of America's recent report [56] on trends in consumer mobility, in 2016 54 percent of Americans used a mobile banking app, whereas in 2017 the figure was up to 62 percent.

2.1.2. Quantifying cyber risk

The representation of the different types of potential losses from cyber events are detailed by the SANS Institute [18] and provided in the appendix of this thesis.

Maynard and Ng [47] propose a research approach to measure cyber risk exposure and potential cyber risk factors. They consider two separate cyber security threat scenarios to measure the propensity of loss of organisations exposed to infected systems. Moreover, their report covers a frequency and severity analysis based on a probability maximum loss model. The idea is to study the different occured losses, through stochastic simulations, by using the data at their disposal. The probabilistic modelling framework relies on existing exposure data from real organisations, as well as on historical loss costs. The stochastic method is used to both model and predict the probability of breaches for a given organisation along with the according loss severities. Their research shows that cyber risk is a recipe for great economic disaster.

The main discoveries regarding the costs brought on by IT security risks include:

- The immediate economic implications of materialised cyber threats can cause a large variety of economic losses, which may heavily deviate from their expected values due to the ambiguity related to cyber risk aggregation [47].
- Cyber attacks are capable of engendering an extremely high amount of insured losses, and a single materialised cyber threat can increase industry loss ratios by 19% for large, and by 250% for extreme events [47].

- The average annual cost derived from cybercrime was $11.7 million a year for companies in 2017, i.e. 62% up from 2012, according to the 2017 Ponemon Institute survey [54].
- Malware and web-based attacks are the most expensive types of cyber attacks, although the costs differ considerably across different countries [54].
- Cybercrime costs are the highest for companies in the financial services sector [54].
- The most costly consequence of a cyber attack is information theft [54].
- The frequency and complexity of attacks increase the cost of cybercrime [54].
- Companies invest the most in cybercrime detection and recovery, while carefully allocating resources towards cost-effective solutions [54].
- The global cost of cybercrime is estimated to double, from $3 trillion up to $6 trillion, within the period of 2015-2021, according to Cybersecurity Ventures [50].

The economic pricetag of cyber attacks has drawn the attention of various IT security specialists recently [50]. Despite the finest and most up-to-date security technology applied on a given component, it may still get compromised by a cyber event. In the fear of a security breach and catastrophic losses, companies have begun to allocate more resources in cyber safety. While the direct loss costs generated by cyber attacks alone are significant, they only represent a small part of a companie's total losses entailed by the malicious cyber event. In fact, the actual costs have been found to extend much further. Losses, such as the loss of trust or reputation, are difficult to quantify and are not often observable right away. Hence, although a company may manage to cover direct financial losses, it is possible that it never fully recovers from the breach [23]. Consequently, investing in cybercrime prevention is the best way to minimize the losses and avoid disastrous consequences.

2.2. Modelling cyber risk

2.2.1. Modelling cyber risk data

The major problem of Internet risks is the fast-paced evolution of the threats, which makes keeping up with an adequate modelling framework even harder. In fact, there are not many sources for cyber risk data, and since the Internet environment is developing rapidly, the information becomes quickly useless. Therefore, it is crucial to have access to updated information in order to obtain more precise data descriptions and accurate risk estimations. The availability of different data sources to obtain information about the prevalence and magnitude of threats, together with the analysis of potential cyber risk scenarios, promote awareness and help in being further prepared against the variety of attacks.

In their paper, Eling and Schnell [21] discuss the main queries associated with cyber risk and cyber insurance. They focus on the concept of cyber risk and on its effects, and go through information on where to extract and how to work on data about cyber risk. According to their study, the lack of cyber risk data is partly caused by the unwillingness of cyber attacks victims to report the incidents. This is logical, since compromised institutions do not want to be labeled as victims of cybercrime. With this being said, to model cyber risks, the paper provides a comprehensive list of both aggregated and raw data sources, along with a brief description of each source. The authors point out that, while the majority of empirical research is based on information about data breaches, a more fruitful way to model cyber risk is to consider the de facto insurance claims, collected by freshly established loss databases, e.g. NetDiligence (2014).

As for the actual modelling of cyber risks, their research [21] advises on using frequency and severity models with high value theory and by prioritising peaks instead of a threshold. Another mentioned method is applying a heavy tail distribution. More specifically, power law and log-normal distributions can be considered to model severity, whereas negative binomial distributions are best suited for the frequency [21]. Furthermore, as already presented in 1.3, copulas constitute an effective tool in modelling nonlinear dependence as well as in dealing with different kinds of distributions. Therefore, they form a good base for modelling aggregated and complex cyber risks.

McQueen, et al. [49] propose a model to estimate how long it takes for a control system with an apparent vulnerability to become compromised by cybercrime. In order to model the random process, it is decomposed as three distinct subprocesses, each corresponding to a different situation and following a different failure probability distribution. The model relies on the assumption that these subprocesses are mutually exclusive, as well as makes simplifying assumptions in the absence of adequate data on vulnerabilities. However, the lack of data may not be such a significant issue, since even if there is data available, it quickly becomes obsolete due to the rapid evolution of the cyber environment [21].

In [49] the subprocesses are first estimated separately. This is followed by the determination of the probability distribution for the complete random process by incorporating the subprocesses. Finally, the expected value of this distribution is estimated by means of a weighted sum of the expectations of each subprocess, with the weights referring to the probabilities of the associated process being operative. Although the model does not require complete information on vulnerabilities and can help in mitigating cyber threats, it fails to consider the dependence among these vulnerabilities. This constitutes an important drawback, as in practice, computer network components are interdependent.

Althoug still lacking, as the number of cyber attacks increases with time, there is a growing amount of data available to model cyber risk. However, in addition to existing data bases about IT risks, some information could also be extracted from online social media (e.g. Facebook, Twitter). In fact, since they carry a lot of information on a considerable number of users, they constitute a valuable source of information, and such data sources are already used in the literature to estimate various types of models, including cyber threats. Lyudmyla et al. [44] describe in detail the methodology behind modelling social networks' data.

2.2.2. Modelling interdependent and correlated cyber risks

As noted in 1.2, the different dependencies among risks introduce several challenges, which in turn complicate the task of accurate model specification. As a result, estimations can be misleading, which then drives entities to misdirect their security investments to unproductive solutions. In other terms, in order to obtain realistic estimates and prevent nonprofitable resource allocation, the nonlinear dependence should be accounted for, when modelling cyber risk. In fact, the key to proper cyber risk management relies on the understanding of the dependence characteristics of the risks. Interdependence and correlation are present in various previous studies (e.g. [14], [32], [41], [51], [58], [67], [68]).

Böhme and Kataria [14] introduce models for correlated IT risks and their implementation, and provide a theoretical approach to model cyber insurance market with respect to correlation (see 1.2.2). They also use honeypot data and propose a modelling framework for empirically estimating the correlation in risk arrival, while taking into account both internal and global correlation. In fact, the process is double-staged and different estimation methodologies are employed for the two types of correlation. Internal correlation is modelled using a Beta-Binomial model (BB), whereas a k-dimensional t-copula is defined for global correlation (k being the number of firms in the insurer's risk portfolio). Given the data structure of honeypot data, however, the number of affected nodes[8] within an organisation is unknown, meaning that the copula cannot be used in this case. Instead, for global correlation, both a Beta-Binomial model and a single factor latent risk model are fitted. The comparison between the models for estimating global correlation suggests that, while the two models account for fat tails, the latent factor model performs better in explaining the correlation in the data [14].

The overall emprical implications in [14] show that an independent Binomial is overperformed by the Beta-Binomial and the single factor latent model, as it understates the tails of the true distribution, hence confirming the presence of correlation in the true distribution. Furthermore, the amplitude of internal correlation is very different depending on the network, and the Beta-Binomial returns smaller coefficients in the case of modelling internal correlation than in the case of global correlation [14].

Hofmann and Ramaj [32] introduce a model for the interdependent cyber network. According to their findings, Internet users do not protect themselves enough against cyber risk. In fact, given the interdependent risk structure of Internet networks, entities with comprehensive cyber risk protection that accounts for the different dependence characteristics ought to be rewarded. This is because, by engaging in thorough cyber safety measures, an entity reduces the overall risk of the network [32].

Öğüt et al. [68] on the other hand, analyse the impact of interconnected IT on the cyber insurance market by comparing a baseline model with independent firms to a model with interdependent

[8] A node is any network connected device characterised by an IP address.

firms. The interdependence is modelled through two symmetric firms, which can either face a direct or an undirect attack, depending on which one of the two gets infected first. Each firm can only affect the probability of direct attacks by self-protection, and the probability of an indirect attack is determined according to the probability of a direct attack in the other firm and the level of interdependence between the two. The results indicate that there is a negative relationship between a firm's incentive to self-protect and cover itself against cyber risks and the degree of interdependence [68].

2.3. Predicting cyber risk

2.3.1. Early warning cyber defense

Sapienza et al. [57] introduce a way to automatically generate warnings of cyber threats by exploiting cybersecurity blogs and darkweb forums. Their system searches through an extensive list of cybersecurity related words as well as through the social media feeds of well established security researchers and white hat hackers[9] looking for different vulnerabilities. It then returns only the relevant words and scans through some darkwed hacking forums to see whether the terms appear on them. At the end, the algorithm generates a warning and reports whether the term is potentially linked to a cyber threat. It provides the number of times the word has been used on Twitter or hacking forums along with the content of the posts mentioning the term.

The method can be used to forecast cyber threats. The case study analysis on Mirai malware (2016) shows that the model could have anticipated the vulnerabilities and organisations could have been better prepared against these attacks. In fact, the underlying algorithm was found to generate warnings as early as 49 days prior to the intrusion. Furthermore, the process was able to alert about the term "mirai" being used on darkweb in between two critical attack concentrations [57].

[9] White hat hackers are IT security professionals, who break into protected computer systems to test their safety and, unlike malicious black hat hackers, use this knowledge in the aim of improving the security of these information systems.

2.3.2. Measuring and predicting the effectiveness of cyber defense

Cyber risks can be reduced, and unnecessary or inefficient security investments avoided, with appropriate protection measures. As the impact of the risk depends on the entity's precautionary behaviour, the determination of efficient cyber defense systems is important in terms of both minimizing the losses and the allocation of security resources. In fact, it has also become of interest to quantify the effect of cyber protection to be able to compare different defence systems and choose an optimal one accordingly. Research on the performance of existing cyber protection facilitates the development and improvement of methods and systems to promote cybersecurity. Xu, et al. [66] apply a copula model for predicting the effectiveness of early warning using data from UCSD CAIDA's network telescope. They model the dependency in a four-dimensional time-series by means of a mixed vine copula model that allows for the adequate representation of their data structure. In fact, it takes into account the number of attacks and victims before and after the early warning mechanism is used. The idea is basically to define the total number of attacks and victims that the early warning prevented.

As presented in 1.3, copulas are useful when representing the joint distribution of differently distributed random variables and their nonlinear relationship. The choice in [66] of a four-dimensional distribution is a logical, since it makes it possible to measure the effectiveness by comparing both, the total number of attacks and the total number of victims, without and inspite of the defense mechanism. Besides, considering attacks and victims separately in the cases where mainly small groups of victims are targeted could lead to an incorrect measure of effectiveness. Furthermore, the four-dimentional time series is a necessity in order to do prediction on the early warning's performance [66]. This being the case, copulas provide an effective solution for modelling the multivariate dynamic dependence structure.

A copula-GARCH (Generalized AutoRegressive Conditional Heteroskedasticity) model

Although copulas constitute a powerful tool when dealing with multivariate distributions, they alone fail to describe data adequately in the presence of high volatility, which justifies the use of a copula-GARCH model. In the literature, copula-GARCH models have typically been applied to financial time series in order to analyse financial markets (e.g. [36], [53], [52], [5], [17]), which are characterized by a high level of volatility. They allow for a comprehensive description of the time varying volatility and volatility clusters, skewness, leptokurtocity and asymmetries as well as the extreme tail dependence structure of financial data [17]. Furthermore, relying on Wold's representation theorem[10], AutoRegressive (AR) as well as AutoRegressive Moving Average (ARMA) models are widely used in finance to predict second order stationary processes. Fitting an ARMA for the conditional mean part in a GARCH model ensures the absence of serial correlation, while the conditional volatility can be modelled by exploiting the heteroskedasticity element in GARCH.

The general theory of copulas and their implementation can be found in the literature (e.g. [1], [22], [62], [13]) as well as the estimation of multivariate GARCH models (e.g. [7], [59], [52]). The modelling and estimation by means of a copula-GARCH method are well detailed in [24], [17]. The method consists in first identifying an appropriate GARCH for fitting the univariate marginals and then defining a suitable copula to model the dependence among the standardized residuals. That is, the marginal distributions of the filtered residuals are fitted with a semi-parametric cumulative distribution function (cdf) using copula functions. The mean part can be modeled as an (ARMA(p,q)) to allow a varying mean [66].

ARMA-GARCH [66]:

$$Y_{j,t} = E\left(Y_{j,t} \middle| \omega_{j,t-1}\right) + \epsilon_{j,t} \,, \qquad j = 1,..,4$$

where $E\left(Y_{j,t} \middle| \omega_{j,t-1}\right)$ is the conditional expectation of $Y_{j,t}$, conditional on the past information $\omega_{j,t-1}$ up to $t-1$, and $\epsilon_{j,t}$ is the error term or innovation of the model.

By construction, the model can also be written in the form of an ARMA(p,q) [66], [24]:

[10] Wold's theorem states that any nondeterministic second order stationary process Y_t can be decomposed as follows: $\forall\ Y_t$ with $E[Y_t] = m_{Y_t}$ and $Cov[Y_t, Y_{t-k}] = \gamma_k$,

$$Y_t = \sum_{j=0}^{\infty} \psi_j a_{t-j} + a_t \,, \qquad \psi_0 \overset{\text{def}}{=} 1 \,, \qquad \sum_{j=1}^{\infty} \psi_j^2 < \infty \,,$$

where ψ_j is the linear filter and $a_t \sim WN(0, \sigma_a^2)$ is a white noise process.

$$Y_{j,t} = \mu_j + \sum_{k=1}^{p} \phi_k Y_{j,t-k} + \sum_{l=1}^{q} \theta_l \epsilon_{j,t-l} + \epsilon_{j,t}\,, \qquad j = 1,..,4\,,$$

where p is the order of the AR part and q the order of the MA part, and $\epsilon_{j,t} = \sigma_{j,t} Z_{j,t}$, with $Z_{j,t}$ the independent and identically distributed innovations for $j = 1,..,4$.

To model the copula pairs between the four time series considered in [66], Xu, et al. propose a mixture copula C between time series denoted U (attacks or victims prior to using early warning) and V (attacks or victims despite using early warning). If C^*denotes a nonexchangeable bivariate parametric copula and $\bar{C}^*$ its survival function, the copula C can be defined as follows:

$$C(u,v) = 0.5C^*(u,v) + 0.5\bar{C}^*(1-u,1-v)$$

The conditional cdf is then: $C_{1|2}(u|v) = 0.5\left[C^*_{1|2}(u|v) - C^*_{1|2}(1-u|1-v) + 1\right]$ and the density: $c(u,v) = 0.5c^*(u,v) + 0.5c^*(1-u,1-v)$. The nonexchangeable bivariate copula C^* can be constructed using a Khoudraji-type copula specification [39] or by following the methodologies in [20], [27].

The idea behind a vine copula is to represent a multivariate copula as a product of bivariate copulas. Aas, et al. [1], and Kurowicka and Cooke [42], introduce modelling frameworks for the applying copula models and provide a comprehensive definition of D-vine copulas. Following the pair-copula approach detailed in [1], an n-dimensional D-vine's density $f(x_1, x_2, \dots, x_n)$ can be decomposed as follows:

$$\prod_{k=1}^{n} f(x_k) \prod_{j=1}^{n-1} \prod_{i=1}^{n-j} c_{i,i+j|i+1,\dots,i+j-1}\{F(x_i|x_{i+1},\dots,x_{i+j-1}), F(x_{i+j}|x_{i+1},\dots,x_{i+j-1})\}\,,$$

where $c_{i,i+j|i+1,\dots,i+j-1}(\cdot)$ is a pair copula density, and j and i denote the trees T_j and their edges respectively. Hence, the four-dimensional D-vine structure employed in [66] can be represented with the following illustration:

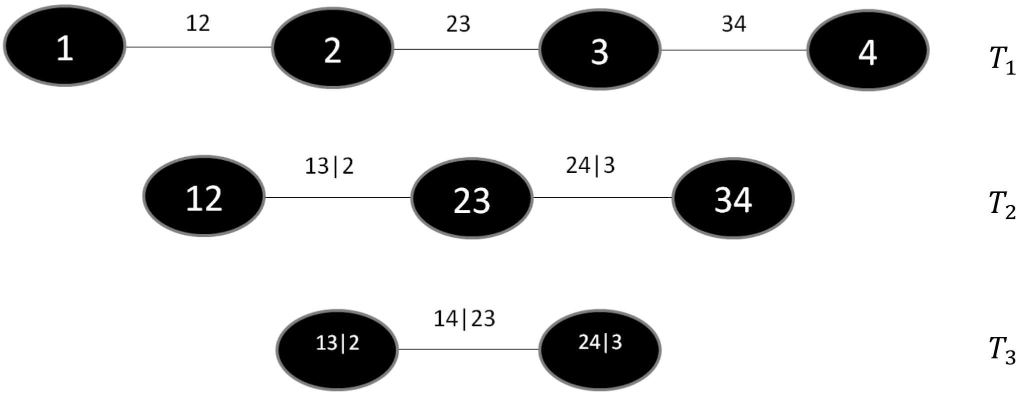


Figure 1. *A four-dimensional D-vine with 3 trees and 6 edges. Each edge (connecting the nodes) can be associated with a pair-copula density, and the edges labels correspond to the subscripts of the copula densities. For example, the edge 14|23 is associated with the copula density $c_{14|23}(\cdot)$ [1].*

Based on the insights in [1], the structure of the D-vine in the four-dimensional case presented in [66] is written as:

$$
\begin{aligned}
c(u_1,u_2,u_3,u_4) = {} & c_{12}(u_1,u_2)\cdot c_{23}(u_2,u_3)\cdot c_{34}(u_3,u_4) \\
& \cdot c_{13|2}\left(C_{1|2}(u_1|u_2), C_{3|2}(u_3|u_2)\right)\cdot c_{24|3}\left(C_{2|3}(u_2|u_3), C_{4|3}(u_4|u_3)\right) \\
& \cdot c_{14|23}\left(C_{1|3}\left(C_{1|2}(u_1|u_2)|C_{3|2}(u_3|u_2)\right), C_{4|3}\left(C_{4|2}(u_4|u_2)|C_{3|2}(u_3|u_2)\right)\right),
\end{aligned}
$$

where:

- $c(u_1,u_2,u_3,u_4)$ represents the joint density of the uniformly distributed random variables U_1, U_2, U_3, U_4
- c_{12} , c_{23} and c_{34} are given by the previously defined density function $c(u,v)$ of the conditional cdf $C_{1|2}(u|v)$

Sampling from the D-vines with uniform marginals [1], [66]:

1. Draw independent $\omega_1, \omega_2, \omega_3, \omega_4$ form $U(0,1)$
2. Set: $u_1 = \omega_1$
3. Set: $u_2 = C_{2|1}^{-1}(\omega_2|u_1)$
4. Set: $v_{2,2} = C_{1|2}(u_1|u_2)$
5. Set: $v_{3,1} = C_{3|1}^{-1}(\omega_3|v_{2,2})$
6. Set: $u_3 = C_{3|2}^{-1}(v_{3,1}|u_2)$
7. Set: $v_{3,2} = C_{2|3}(u_2|u_3)$
8. Set: $v_{3,4} = C_{1|3}(v_{2,2}|v_{3,2})$
9. Set: $v_{4,1} = C_{4|1}^{-1}(\omega_4|v_{3,4})$. If C_{14} is independent, then simply $v_{4,1} = \omega_4$.
10. Set: $v_{4,1} = C_{4|2}^{-1}(v_{4,1}|v_{3,2})$
11. Set: $u_4 = C_{4|3}^{-1}(v_{4,1}|u_3)$
12. Return the output: (u_1, u_2, u_3, u_4)

In order to forecast the effectiveness of early warning, the joint distribution of the time series at $t + 1$ can be sampled using a Monte Carlo simulation. Then the simulated copula structured outputs are transformed into times series predictions of the form: $\hat{y}_{i,t+1} = \hat{\mu}_{i,t+1} + \hat{F}_i^{-1}(u_{i,t+1})\hat{\sigma}_{i,t+1}$, $i = 1, . . ,4$, with $\hat{\mu}_{i,t+1}$ the predicted value of the mean and $\hat{\sigma}_{i,t+1}$ the predicted value of the standard deviation, and $\hat{F}_i^{-1}(\cdot)$ the inverse function of a skewed student-t distribution. Finally, the effectiveness can be predicted for $t+1$ by defining the conditional probability: $p(t) = P(atta(t), vica(t)|attb(t), vicb(t))$ [66], where:

- $atta(t) \in A'$ is the time series representing the number of attacks the early warning failed to block
- $vica(t) \in V'$ is the time series representing the number of victims touched by the attacks the early warning failed to block
- $attb(t) \in A$ is the time series representing the number of attacks that occured before using the early warning cyber defense
- $vicb(t) \in V$ is the time series representing the number of victims touched by the attacks before using early warning cyber defense

3. Cyber insurance market

Although insurance is a very common way to deal with risk, the market of cyber insurance has not really kicked off yet. The market for cyber insurance is relatively small compared to other branches of insurance. It is for only about 20 years that insurance has been perceived as a relevant cyber risk management tool [43]. The low succes of cyber insurance may be explained for one by its sensitive nature. For instance, as in any form of insurance, the person desiring to be insured needs to provide the insurer with somewhat delicate details, which ironically might even put the entity into danger. Indeed, in order to get coverage it is necessary to provide the insurer with confidential information, which compromises the privacy of the entity and creates another vulnerability. For instance, if an insurance company is subject to a data breach, all the information it holds on its clients is at risk. Moreover, as discussed in chapter 1, the challenges related to insuring cyber risk limit the supply of cyber insurance in itself. However, insurers have several means at their disposal for monitoring the behaviour of their clients, whereas how can the policy holders be sure whether the insurance companies themselves employ sufficient security measures in order to keep their clients' data safe?

Another possible reason for why the cyber insurance market is not flourishing is the policy holders' difficulty to justify their losses to the insurer [69]. Because of the asymmetry of information and the fear of fraudulent claims, insurers require strong proof regarding the source and extent of the losses and might wrongly deny indemnisation or part of it in the absence of satisfactory evidence from the insured. The detection of malware is not easy and they can induce a considerable amount of damage before noticed. In addition, the losses from cyber attacks can be hard to show to be of importance (e.g. an invention whose scope and value have not yet been defined) and are often intangible (e.g. loss of reputation, loss of competivity). This makes it even harder, on the one hand for insurers to distinguish the pure effect of the incurred intrusion, and on the other hand, for policy holders to obtain full and legitimate compensation for the losses.

Furthermore, a rather simple explanation for the immature market is that cyber risk is underestimated. The poor understanding of exposures, along with the lack of knowledge on cyber coverage options, are still reflected on the size of the market. Nevertheless, attitudes are changing as cyber attacks are becoming more prominent and cybersecurity more regulated. This chapter provides a quick review of the current state of the market, and more specifically, its main actors.

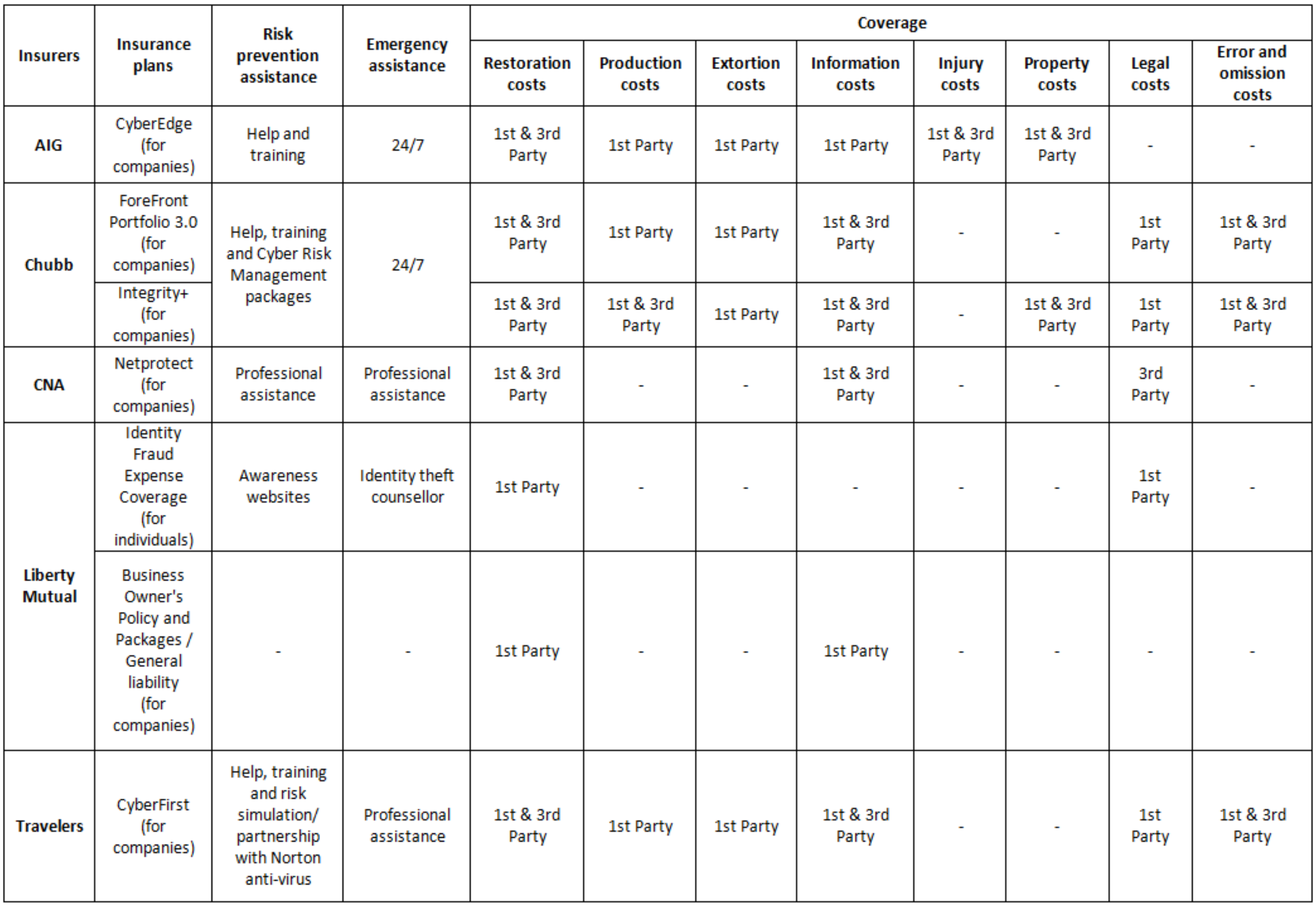
3.1. Cyber insurance supply

The value of the cyber insurance market is estimated to be around 3 or 3.5 billion US dollars, though it is expected to grow up to 7.5 billion by the year 2020 [47], [60]. The rising market shows promising to insurers, and despite the various difficulties and uncertainty regarding insuring cyber risk, insurance companies are interested in the growing market opportunities.

Before there exist any proper cyber insurance policies, part of the losses yielding from cyber risk were accounted for in traditional insurance contracts [9]. However, the supply of cyber coverage has since broadened, as well as the variety of offered products. For instance, additional aspects have come to cover losses generated by data breaches and losses brought on with the interruption of activity that were not included in the traditional policies. Moreover, it is worth mentioning that the current cyber insurance coverage often includes some assistance servises, which are at disposal for the insureds, who need them. In particular, cyber insurance contracts typically include coverage for the following types of costs [60]:

- the costs of risk evaluation by a computer expert
- the costs of incident and crisis mangement
- data construction costs
- the costs of repairing an infected system
- costs of operating losses
- costs of administrative inquiry
- notification costs
- third party damages caused by data disclosure
- cost of a lawyer
- appeal costs

There are several rankings, which provide a list of the most important suppliers of cyber insurance (e.g. [7], [35], [47], 0). Based on those rankings, I chose five cyber insurance offering companies and summarised their details in the table below, in order to facilitate comparison between them.



Insurers	Insurance plans	Risk prevention assistance	Emergency assistance	Coverage							
				Restoration costs	Production costs	Extortion costs	Information costs	Injury costs	Property costs	Legal costs	Error and omission costs
AIG	CyberEdge (for companies)	Help and training	24/7	1st & 3rd Party	1st Party	1st Party	1st Party	1st & 3rd Party	1st & 3rd Party	-	-
Chubb	ForeFront Portfolio 3.0 (for companies)	Help, training and Cyber Risk Management packages	24/7	1st & 3rd Party	1st Party	1st Party	1st & 3rd Party	-	-	1st Party	1st & 3rd Party
	Integrity+ (for companies)			1st & 3rd Party	1st & 3rd Party	1st Party	1st & 3rd Party	-	1st & 3rd Party	1st Party	1st & 3rd Party
CNA	Netprotect (for companies)	Professional assistance	Professional assistance	1st & 3rd Party	-	-	1st & 3rd Party	-	-	3rd Party	-
Liberty Mutual	Identity Fraud Expense Coverage (for individuals)	Awareness websites	Identity theft counsellor	1st Party	-	-	-	-	-	1st Party	-
	Business Owner's Policy and Packages / General liability (for companies)	-	-	1st Party	-	-	1st Party	-	-	-	-
Travelers	CyberFirst (for companies)	Help, training and risk simulation/ partnership with Norton anti-virus	Professional assistance	1st & 3rd Party	1st Party	1st Party	1st & 3rd Party	-	-	1st Party	1st & 3rd Party

***Table 1.** Five higly quoted cyber insurance providers, each listed in the top cyber coverage choices of at least two recent rankings, and the products offered by them.*

As for the cyber risk reinsurance market, some reinsurance companies cover part of the risk faced by cyber insurers. The most important providers of cyber reinsurance include:

- Munich Re (Munich Reinsurance Co.) [79]
- NAS Cyber Liability (NAS Insurance) [80]
- Partner Re (PartnerRe Ltd.) [81]
- Everest Reinsurance Company (Everest Re Group) [82]
- Trans Re (Transatlantic Holdings, Inc.) [83]

3.2. Cyber insurance demand

According to the Betterley report [9], the demand for cyber insurance is not limited to large companies or only entities with important cyber risk exposures. In fact, an increasing number of small and medium size companies are buying cyber coverage [9], although there still remains a significant lack of knowledge about cyber risk among these types of companies [14]. The market is expanding, in particular, in the health care sector and among companies of smaller size, who have recently become aware of their potential liabilities. Many of them seek cyber insurance, since it is imposed by other entities, whom they do business with. Furthermore, small and medium companies find themselves more and more in situations, where they are faced with liability for an unlimited amount of losses. These business agreements between companies, requiring coverage for IT risks, constiute a significant motivation for purchasing cyber insurance [9].

In their study on cyber insurance, Böhme and Kataria [14] analyse the demand for cyber coverage through firms' decisions to buy insurance. They point out the ambiguity of whether the premiums assigned to the insureds are economically reasonable. As cyber risks tend to have a correlated nature making the estimation of expected losses more complicated, it is difficult to say if the premiums paid on the market are too high [14], [60]. After first investigating from the insurer's perpective the premium they would need to set to cover risks, the reasearch [14] examines the utility for a firm with and without insurance coverage to conclude on the firm's propensity to purchase cyber insurance. Their results suggest that firms tend to choose insurance when the risk aversion is higher but would rather not insure themselves in the presence of low internal correlation and probability of failure. This makes sense as, in that case, firms would not necessarily need to transfer their risk to a third party [14].

A recent report from Le Club des Juristes [60] finds that the demand for cyber insurance is reduced due to the improper understanding of Internet risks and cyber coverage. Many companies still underestimate the threat and fail to correctly identify their predisposing factors, and especially smaller companies are unaware of the availability and versatility of different cyber insurance policies. In fact, they tend to have a lack of technical knowledge and legal expertise within their IT risk management, leaving them with insufficient cyber security infrastructure. Fortunately, the report also lists ten recommendations to better address cyber risk insurance. The list constitutes a set of rules that highlight the importance of awareness, and of further monitoring, in order to better apprehend past incidents, as well as a clearer vision of the available cyber risk managemet solutions [60].

To illustrate cyber insurance demand, here are some figures reported in [60]:

- The American market represents about 85 to 90 percent of the annual premiums, whereas Europe represents only 5 to 9 percent of the global cyber insurance market.
- 73 percent of the surveyed French industrial companies did not have cyber coverage at the end of the year 2016, 32 percent of which, however, had an intention to cover themselves within the twelwe following months.
- 79 percent of French companies having less than 250 employees and 60 percent of the having more than 250 employees were not insured against cyber risk.

Cyber risk has certainly become an integral part of companies' risk assessment. Whether companies indeed protect themselves to a sufficient extent is an interesting question, especially form the viewpoint of the companie's clients and shareholders. The 2017 IBM X-Force Report [37] points out the importance of human factor in cybersecurity. According to the report, 70 percent of the compromised records tracked by IBM X-Force in 2017 were exposed due to human errors or mistakes in infrastructure configurations. In order to support companies and other entities in cyber risk safety, HSBC UK's cybercrime overview gives four rules of thumb in form of an acronym [71]:

1. **S**ecure. Keep digital and personal property well secured from cybercrime.
2. **A**lert. Be aware and careful, and apply security policies across all processes.
3. **F**unctioning. Make sure the systems are always up to date and operational.
4. **E**ducated.Provide training, guidance and support for the members of the staff.

Conclusion

The aim of this thesis was to investigate the insurance for cyber risk in the economic and financial contex, as well as to review the different modelling insights applied in literature to assess IT risks. The unique and fast-paced nature of network threats intrigues and frustrates the research community. The scarcity of data sources and the one of a kind dependency structure of cyber risks have encouraged several researchers to tackle with the task of analyzing and modelling them.

Cyber risk has brought on both challenges and opportunities. While cybercrime is becoming a customary problem, the market for cyber insurance and reinsurance are gaining ground. Attacks are more and more prominent, and the general awareness of the risk is increasing. Furthermore, the growing amount of regulation and tightened law enforcements force different organisations to stay up to date on cyber safety issues. As all this is happening very fast, companies and other entities have a strong need for guidance and risk reduction, which explains the important role of cyber coverage.

The rapid technological advances and the quickly changing cyber environment have led to a cat and mouse play between IT security experts and cybercriminals. Malicious actors on the Internet exploit any new vulnerabilities they may find in emerging network structures, while security professionals struggle in filling the loopholes. It is left to be seen, whether the cat can ever completely catch the mouse.

References

[1] K. Aas, C. Czado, A. Frigessi and H. Bakken (2009), "Pair-copula constructions of multiple dependence", Insurance: Mathematics and Economics, 44(2), pp. 182-198, https://doi.org/10.1016/j.insmatheco.2007.02.001

[2] I. A. Adeleke, A. Ibiwoye and F. F. Olowokudejo (2011), "Cyber risk Exposure and Prospects for Cyber Insurance", International Journal of Management and Business Research, 1(4), pp. 221-230

[3] M. Agrawal and S. Shivendu (2016), "Cyber Insurance at USF", Journal of Information Technology Education: Discussion Cases, Informing Science Institute, 5(3), Eds: T. G. Gill

[4] G. A. Akerlof (1970), "The Market for "Lemons": Quality Uncertainty and the Market Mechanism", The Quarterly Journal of Economics, 84(3), pp. 488-500

[5] R. Aloui, M. S. B. Aïssa, D. K. Nguyen (2013), "Conditional dependence structure between oil prices and exchange rates: A copula-GARCH approach", Journal of International Money and Finance, 32, pp. 719-738, https://doi.org/10.1016/j.jimonfin.2012.06.006

[6] L. Bailey (2014), "Mitigating Moral Hazard in Cyber-Risk Insurance", Journal of Law & Cyber Warfare, 3(1), pp. 1-42, https://ssrn.com/abstract=2424958

[7] T. Ball (2018), "Top 5 cyber insurance providers offering the best cover againsr attack", Computer Business Review January 2018, https://www.cbronline.com/list/top-5-cyber-insurance-providers

[8] L. Bauwens, S. Laurent and J. V. K. Rombouts (2006), "Multivariate GARCH models: a survey", Journal of Appled Econometrics, 21(1), pp. 79-109, https://doi.org/10.1002/jae.842

[9] R. S. Betterley, LIA (2018), "Cyber/Privacy Insurance Market Survey – 2018", The Betterley Report, https://www.irmi.com/docs/default-source/publication-tocs/betterley-report---cyber-risk-market-survey-june-2018-summary.pdf

[10] C. Biener, M. Eling, J. H. Wirfs (2015), "Insurability of Cyber Risk: An Empirical Analysis", Geneva Papers on Risk and Insurance: Issues and Practice, 40(1), pp. 131-158, Institute of Insurance Economics (I.VW-HSG), https://doi.org/10.1057/gpp.2014.19

[11] J. Bolot and M. Lelarge (2008), "Cyber Insurance as an Incentive for Internet Security", Seventh Workshop on the Economics of Information Security (WEIS), https://doi.org/10.1007/978-0-387-09762-6_13

[12] L. Bonner (2012), "Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches", Washington University Journal of Law & Policy, 40(1), https://openscholarship.wustl.edu/law_journal_law_policy/vol40/iss1/7

[13] E. C. Brechmann and U. Schepsmeier (2013), "CDVine: Modeling Dependence with C- and D-Vine Copulas in R", Journal of Statistical Software, 52(3), https://doi.org/10.18637/jss.v052.i03

[14] R. Böhme and G. Kataria (2006), "Models and Measures for Correlation in Cyber-Insurance", Workshop on the Economics of Information Security (WEIS)

[15] R. Böhme and G. Kataria (2006), "On the Limits of Cyber-Insurance", Trust and Privacy in Digital Business, Lecture Notes in Computer Science, 4083, pp. 31-40, Eds: S. Fischer-Hübner, et al., Springer-Verlag, Berlin, Heidelberg, https://doi.org/10.1007/11824633_4

[16] R. Böhme and G. Schwartz (2010), "Modeling Cyber-Insurance: Towards A Unifying Framework", Working Paper, Workshop on the Economics of Information Security (WEIS), Harward, https://www.econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf

[17] Q. Chen, D. Wang and M. Pan (2015), "Multivariate Time-Varying G-H Copula GARCH Model and Its Application in the Financial Market Risk Measurement", Mathematical Problems in Engineering, http://dx.doi.org/10.1155/2015/286014

[18] J. D. Christopher (2017), "Incentivizing Cyber Security: A Case for Cyber Insurance", SANS Institute, InfoSec Reading Room, https://www.sans.org/reading-room/whitepapers/riskmanagement/paper/37845

[19] J. R. Conrad (2005), "Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations, University of Idaho, https://pdfs.semanticscholar.org/6b83/493eb062e447249ac80e48a99a78143e81f4.pdf

[20] F. Durante (2009), "Construction of non-exchangeable bivariate distribution functions", Statistical Papers, 50(2), pp. 383-391, Springer-Verlag, https://doi.org/10.1007/s00362-007-0064-5

[21] M. Eling and W. Schnell (2016), "Ten Key Questions on Cyber Risk and Cyber Risk Insurance", The Geneva Association, International Association for the Study of Insurance Economics

[22] P. Embrechts, F. Lindskog and E. J. Mcneil (2001), "Modelling Dependence With Copulas and Applications to Risk Management", https://doi.org/10.1016/B978-044450896-6.50010-8

[23] N. Eubanks (2017), "The True Cost Of Cybercrime For Bussinesses", Forbes, https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#4ed55ac34947

[24] C. Francq and J.-M. Zakoïan (2004), "Maximum likelihood estimation of pure GARCH and ARMA-GARCH processes", Bernouilli, 10(4), pp. 605-637, https://doi.org/10.3150/bj/1093265632

[25] V. Garg and L. J. Camp (2012), "End User Perception of Online Risk under Uncertainty", 45th Hawaii International Conference on System Sciences, IEEE, https://doi.org/10.1109/HICSS.2012.245

[26] V. Garg and L. J. Camp (2015), "Cars, Condoms, and Facebook", Eds: Y. Desmedt, Information Security, Lecture Notes in Computer Science, 7807, Springer, Cham, pp. 280-289, Springer International Publishing, https://doi.org/10.1007/978-3-319-27659-5_20

[27] C. Genest and L.-P. Rivest (1993), "Statistical Inference Procedures for Bivariate Archimedean Copulas", Journal of the American Statistical Association, 88(423), pp. 1034-1043, https://doi.org/10.1080/01621459.1993.10476372

[28] L. A. Gordon, M. P. Loeb and T. Sohail (2003), "A Framework for Using Insurance for Cyber-Risk Management", Communications of the ACM, 46(3), pp. 81-85, https://doi.org/10.1145/636772.636774

[29] G. Heal and H. Kunreuther (2006), "Modeling Interdependent Risks", Risk Analysis 2007, 27(3), pp. 621-634, https://doi.org/10.1111/j.1539-6924.2007.00904.x

[30] D. Helbing (2013), "Globally networked risks and how to respond", Nature 497(May), pp. 51-59, Macmillan Publishers Limited, https://doi.org/10.1038/nature12047

[31] H. S. B. Herath and T. C: Herath (2011), "Copula-based actuarial model for pricing cyber-insurance policies", Insurance Markets and Companies: Analyses and Actuarial Computations, 2(1), https://ssrn.com/abstract=1771983

[32] A. Hofmann and H. Ramaj (2011), "Interdependent risk networks: the threat of cyber attack", International Journal of Management and Decision Making, 11(5-6), pp. 312-323, https://doi.org/10.1504/IJMDM.2011.043406

[33] D.-L. Huang, P.-L. Rau and G. Salvendy (2010), "Perception of information security", Behaviour & Information Technology, 29(3), pp. 221-232, https://doi.org/10.1080/01449290701679361

[34] D.-L. Huang, P.-L. P. Rau, G. Salvendy, F. Gao and J. Zhou (2011), "Factors affecting perception of information security and their impacts on IT adoption and security practices", International Journal of Human-Computer Studies, 69(12), pp. 870-883, https://doi.org/10.1016/j.ijhcs.2011.07.007

[35] J. Hunt (2018), "Top Companies Offering Cyber Insurance", The Balance, https://www.thebalance.com/top-companies-offering-cyber-insurance-4171528

[36] E. Jondeau and M. Rockinger (2006), " The Copula-GARCH model of conditional dependencies: An international stock market application", Journal of International Money and Finance, 25(5), pp. 827-853, https://doi.org/10.1016/j.jimonfin.2006.04.007

[37] K. Kane (2018), "IBM X-Force Report: Fewer Records Breached In 2017 As Cybercriminals Focused On Ransomware And Destructive Attacks", IBM News Room, https://newsroom.ibm.com/2018-04-04-IBM-X-Force-Report-Fewer-Records-Breached-In-2017-As-Cybercriminals-Focused-On-Ransomware-And-Destructive-Attacks

[38] J. P. Kesan, R. P. Majuca, W. J. Yurcik (2005), "Cyberinsurance As A Market-Based Solution to the Problem of CyberSecurity – A Case Study", University of Illinois at Urbana-Champaign, https://pdfs.semanticscholar.org/fbac/fbf013bae9077165280e1da04438d0b0c1d8.pdf

[39] A. Khoudraji (1995), "Contributions à l'étude des copules et à la modélisation de valeurs extrêmes bivariées", Ph.D. thesis, University of Laval

[40] H. Kuchler (2017), "Cost of cyber crime rises rapidly as attacks increase", Financial Times, https://www.ft.com/content/56dae748-af79-11e7-8076-0a4bdda92ca2

[41] H. Kunreuther and G. Heal (2003), "Interdependent Security", Journal of Risk and Uncertainty, 26(2-3), pp. 231-249, Kluwer Academic Publishers, https://doi.org/10.1023/A:1024119208153

[42] D. Kurowicka and R. Cooke (2004), "Distribution-free continuous Bayesian belief nets", https://doi.org/10.1142/9789812703378_0022

[43] J. Loveland (2017), "Cyber Insurance – "I don't think it means what you think it means", RSA Conference 2017, San Francisco Feb 13-17, Moscone Center, https://www.rsaconference.com/writable/presentations/file_upload/grc-t10-cyber-insurance_i-do-not-think-that-word-means-what-you-think-it-means.pdf

[44] K. Lyudmyla, R. Tamara and C. Anders (2017), "Detecting cyber threats through social network analysis: short survey", SocioEconomic Challenges, 1(1), pp. 20-34, https://arxiv.org/abs/1805.06680

[45] R. P. Majuca, W. Yurcik, J. P. Kesan (2006), "The Evolution of Cyberinsurance", University of Illinois at Urbana-Champaign, https://arxiv.org/abs/cs/0601020

[46] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, A. Yautsiukhin (2017), "Cyber-insurance survey", Article in Press, Computer Science Review, http://dx.doi.org/10.1016/j.cosrev.2017.01.001

[47] R. Marvin (2018), "What Is Cyber Insurance and Should You Get It?", PCMag, https://www.pcmag.com/feature/358453/what-is-cyber-insurance-and-should-you-get-it

[48] T. Maynard (Lloyd's) and G. Ng (Cyence) (2017), "Counting the cost – Cyber exposure decoded", Emerging Risks Report 2017, Technology

[49] M. A. McQueen, W. F. Boyer, M. A. Flynn and G. A. Beitel (2005), "Time-To-Compromise Model For Cyber Risk Reduction Estimation", Quality of Protection Workshop, eds: D. Gollmann, F. Massacci, A. Yautsiukhin, Advances in Information Security, 23, pp. 49-64, Springer, Boston, MA, https://doi.org/10.1007/978-0-387-36584-8_5

[50] S. Morgan (Editor-in-Chief) (2017), "Cybercrime Damages $6 Trillion by 2021", Cybersecurity Ventures, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[51] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, S. K. Sadhukhan (2013), "Cyber-risk decision models: To insure IT or not?", Decision Support Systems, Elsevier B. V., http://dx.doi.org/10.1016/j.dss.2013.04.004

[52] A. K. Nikoloulopoulos, H. Joe and H. Li (2010), "Vine Copulas With Asymmetric Tail Dependence and Applications to Financial Return Data", Computational Statistics & Data Analysis, 56(11), pp. 3659-3673, https://doi.org/10.1016/j.csda.2010.07.016

[53] A. J. Patton (2009), "Copula-Based Models for Financial Time Series", Eds: T. Mikosch, J. P. Kreiβ, T. Andersen, Hanbook of Financial TIme Series, Springer, Berlin, Heidelberg, https://doi.org/10.1007/978-3-540-71297-8_34

[54] J. Plunkett (2018), "Taking the Wind out of Cyber Risk", Swiss Re, blog post on Linked in, https://www.linkedin.com/pulse/taking-wind-out-cyber-risk-jayne-plunkett/?hootPostID=496bdf873778b90fd9eade032aea4935

[55] Ponemon Institute (2017), "Cost of cyber crime – Insights on the security investments that make a difference", Ponemon Institute LLC jointly developed with Accenture,

https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[56] B. Riess (2017), "Bank of America Trends in Consumer Mobility Report", https://newsroom.bankofamerica.com/press-kits/bank-america-trends-consumer-mobility-report

[57] A. Sapienza, A. Bessi, S. Damodaran, P. Shakarian, K. Lerman and E. Ferrara (2018), "Early Warnings of Cyber Threats in Online Discussions", IEEE International Conference on Data Mining Workshops (ICDMW), pp. 667-674, 2017, https://arxiv.org/pdf/1801.09781.pdf

[58] W. Shim (2010), "An Analysis of IT Security Management Strategies in the Presence of Interdependent Security Risk", ITERA, The 9th Annual Conference on Telecommunications and Information Technology, 2011

[59] A. Silvennoinen and T. Teräsvirta (2008), "Multivariate GARCH Models", CREATES Research Paper, https://doi.org/10.2139/ssrn.1148139

[60] B. Spitz, et al. (2018),"Report: Insuring Cyber Risk", Cyber Risk Commission Report, Le Club des Juristes, https://www.leclubdesjuristes.com/wp-content/uploads/2018/01/cdj_rapport_cyber-risk_janvier-2018_uk_web.pdf

[61] M. Sun (2018), "Why Europe's Cyber Insurance Windfall Hasn't Happened", The Wall Street Journal, https://www.wsj.com/articles/why-europes-cyber-insurance-windfall-hasnt-happened-1529496000?mod=e2tw

[62] P. K. Trivedi and D. M. Zimmer (2005), "Copula Modeling: An Introduction for Practioners", Foundations and Trends in Econometrics, 1(1), pp. 1-111, https://doi.org/10.1561/0800000005

[63] P. van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen and P. Kusev (2017), "Risk perceptions of cyber-security and precautionary behaviour", Computers in Human Behaviour, 75(October), pp. 547-559, https://doi.org/10.1016/j.chb.2017.05.038

[64] B. Spitz et al. (2018), "Insuring Cyber Risk – Report from the Club des Juristes", Cyber risk commission report, January 2018, Le club des juristes, https://www.leclubdesjuristes.com/wp-content/uploads/2018/01/cdj_rapport_cyber-risk_janvier-2018_uk_web.pdf

[65] J. Wiley & Sons Ltd. (2008), "Encyclopedia of Quantitative Risk Analysis and Assessment", https://doi.org/10.1002/9780470061596

[66] M. Xu, L. Hua and S. Xu (2017), "A Vine Copula Model for Predicting the Effectiveness of Cyber Defense Early-Warning", Technometrics, 59(4), pp. 508-520, https://doi.org/10.1080/00401706.2016.1256841

[67] X. Zhao, L. Xue, A. B. Whinston (2009), "Managing Interdependent Information Security Risks: A Study of Cyberinsurance, Managed Security Service and Risk Pooling", Journal of Management Information Systems, 30(1), pp.123-152, 2013, https://doi.org/10.2753/MIS0742-1222300104

[68] H. Öğüt, N. Menon and S. Raghunathan (2005), "Cyber Insurance and IT Security Investment: Impact of Interdependence Risk", WEIS, http://infosecon.net/workshop/pdf/56.pdf

[69] H. Öğüt, S. Raghunathan, N. Menon (2010): "Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection", Society for Risk Analysis, 31(3), pp. 497-512, 2011, https://doi.org/10.1111/j.1539-6924.2010.01478.x

[70] "The Top 5 Cyber Insurance Carriers in the Market", CyberPolicy, https://cyberpolicy.com/cybersecurity-education/the-top-5-cyber-insurance-carriers-in-the-market

[71] Cybercrime – an overview", Cyber Aware, HSBC UK, https://www.business.hsbc.uk/en-gb/cybercrime

[72] https://www.aig.com/business/insurance/cyber-insurance?cmpid=ic/d/ps/go/Google_Cyber//aig///

[73] https://www.libertymutual.com/identity-theft-insurance

[74] https://business.libertymutualgroup.com/business-insurance/coverages/business-owners-policy-packages

[75] https://www.cna.com/web/guest/cna/ps/products/ct-anycyberliabilityprodml/!ut/p/b1/hZHJzoNGEISf5X8A_wwM63HYYTD7YnNBNmZfDMYGm6ePo0TKKUnfulWqan1FpMSJSMfL2lSXZ3MfL_2fe8pmNMA4tOiIMiFkAHI0QJM2pjANiYQ4jZFgB7y3KS54FofqbdomIBM3XU_tm64m6nroOrZDrJUOE1ghaY-qWtR2rTlno

[76] https://www.travelers.com/cyber-insurance

[77] https://www2.chubb.com/us-en/business-insurance/forefront-portfolio-3-0-cybersecurity-insurance.aspx

[78] https://www2.chubb.com/us-en/business-insurance/integrity-by-chubb.aspx

[79] https://www.munichre.com/en/reinsurance/business/non-life/cyberrisks/index.html

[80] http://nasinsurance.com/wp-content/uploads/2017/07/NAS-Cyber-Reinsurance-Brochure.pdf

[81] https://partnerre.com/risk-solutions/cyber-risk/

[82] https://www.everestre.com/Reinsurance/Canada/Alternative-Risk-Solutions

[83] https://www.transre.com/what-we-do/lines-of-business/treaty/cyber/

APPENDIX: Representation of potential losses caused by cyber events

TYPE OF DAMAGE	FIRST PARTY DAMAGES	THIRD PARTY DAMAGES
FINANCIAL DAMAGES	• response costs • legal expenses • revenue losses • expenses from the restoration of lost data • cyber extortion expenses • losses due to stolen intellectual property	• consequential revenue losses • restoration expenses • legal expenses • credit monitoring costs
PHYSICAL DAMAGES	• mechanical breakdown of the first party's equipment • destruction or damage to the first party's facilities • environmental cleanup of the first party's property • revenue losses from business interruption • personal injury to the first party	• mechanical breakdown of a third party's equipment • destruction or damage to a third party's facilities • environmental cleanup of a third party's property • personal injury to a third party

source: SANS Institute [18]