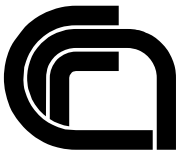

Consiglio Nazionale delle Ricerche

A Survey on Cyber-Insurance

A. Marotta, F. Martinelli, S. Nanni, A. Yautsiukhin

IIT TR-17/2015

Technical Report

Novembre 2015

Istituto di Informatica e Telematica

A Survey on Cyber-Insurance

Angelica Marotta[*], Fabio Martinelli[†] and Artsiom Yautsiukhin[‡]

Instituto di Informatica e Telematica,
Consiglio Nazionale delle Richerce,
Pisa, Italia

Stefano Nanni[§]

Unipol Gruppo Finanziario S.p.A.
Bologna, Italy

Abstract

Cyber insurance is a young and rapidly developing area which draws more and more attention of practitioners and researchers. Insurance, an alternative way to deal with residual risks (next to simple risk acceptance), was only recently applied to cyber world. The immature cyber insurance market faces a number of unique challenges on the way of its development.

In this paper we summarise the basic knowledge about cyber insurance available so far from both market and scientific perspectives. We provide a common background explaining basic terms and formalisation of the area. We discuss the issues which make this type of insurance unique and show how different technologies are affected by these issues. We compare the available scientific approaches to analysis of cyber insurance market and summarise their findings with a common view. Finally, we propose directions for further advances in the research on cyber insurance.

[*]Electronic address: angelica.marotta@iit.cnr.it
[†]Electronic address: Fabio.Martinelli@iit.cnr.it
[‡]Electronic address: artsiom.yautsiukhin@iit.cnr.it; Corresponding author
[§]Electronic address: Stefano.Nanni@unipolsai.it

1 Introduction

In recent years there has been a growing interest to cyber risk and it is considered among the most difficult issues to deal with as cyber risk could lead to serious impact on businesses and societies [51]. The expansion of information technology in business and in everyday reality through the spread of social networks, mobile devices, wireless technologies and cloud services has led to increased vulnerability. Many companies are starting to consider cyber security as a larger business risk and, as a consequence, they are looking for methods to assure the continuity of financial operations in case of cyber attacks [119].

In spite of the wide application of security measures, the losses due to breaches are still extremely high [62]. The study of cyber risk conducted by March in 2013 revealed, that 54% of the interviewed organisations have been a subject of a cyber attack in the last 3 years (when 17% of respondents was not able to answer the question). Furthermore, according to the study commissioned and managed by European Network and Information Security Agency (ENISA) [47], the average cost per breach based on data from underwriters was US$2.4m. A research conducted by Ponemon Insitute [119] reveals that the average financial impact to companies due to a cyber incident was $9.4 million. The average cost per a compromised record is assessed to be $188 according to Ponemon Insitute [119] or $107.14 according to NetDiligence [58]. Thus, it is impossible to mitigate cyber risks completely, while the possible impact becomes higher with higher dependence of business and society on information technologies. Although security countermeasures and practices are important, risk managers should also look for other approaches to deal with residual cyber risks.

One of the alternative approaches in dealing with residual risk is risk transfer, which in most cases means insurance [56, 94, 53, 14, 17]. Starting since 1998 [118, 77, 88] cyber insurance policies became more and more popular on the market. Global surveys [49, 51] and books [144] on insurance consider cyber risks insurance as an important component of risk management programs. More than 50 insurers now provide cyber insurance policies from US, Bermuda and London markets [2, 99]. The gross written premium in US is predicted to be 2,75 billion in 2015 [23] and 150 million in Europe, rising from 50 to 100 per cent annually (prediction for 2014) [76].

Apart from the primary ability to transfer cyber risk and smooth the impact for organisations, insurance in general, and cyber insurance, in particular, is assumed to have additional desirable impact. First and the foremost advantage of insurance is the possibility to provoke organisations to increase investments in its protection, in order to reduce the premium [142, 100, 88, 126, 11]. Next, cyber insurance is believed to improve the societal welfare by improving the overall level of cyber protection [88]. Third, cyber insurance (premiums, in particular) may serve as an indicator of the quality of protection [100]. Last but not least, cyber insurance may lead to new and more advanced standards in cyber security.

Scientific community also moves hand to hand with practical applications

of cyber insurance. The community is mostly focused on the ways to establish insurance contract and analyse impact of difference pricing strategies on the market [14, 26, 150, 106, 85, 134, 128, 113, 98, 123]. The primary focus of researches is on the issue of interdependency of security, one of the peculiarities of cyber risks. The models and approaches, used by the researches are quite similar and it is often hard to spot the key difference between them, especially, when this key difference is not explicitly stated. Furthermore, the mathematics used in the papers is relatively advanced and authors are constrained to provide only limited amount of details with the narrow focus on the considered problem. In this survey we are going to present the basic formalisation to provide the necessary background for the comprehensive understanding of the basic concepts of cyber insurance.

In the past there were several comprehensive studies, which, although were not called "surveys", provided extensive analysis of available literature and marketing practices for the time when they were released. R. Majuca, et. al [88] provided an overview on evolution of cyber insurance by 2005. The study was mostly focused on the market analysis and provided high level discussion of basic problems (e.g., moral hazard). R. Böhme and G. Schwartz [28] provided a unified approach for cyber insurance in 2010, glueing together different aspects of cyber insurance and indicating the approaches of different researches dealing with these aspects. In contrast to these works, the primary focus of this paper is on *surveying* the existing literature on cyber insurance. Our analysis of the scientific literature not only increases the number of considered approaches (taking into account the most recent ones), but also helps to systematise the results achieved by the researchers, rather than simply the problems considered. Such analysis helped us to find the situations, where authors came to the same conclusions and where the authors disagree and further research is required. In other words, our paper does not repeat the existing works, but provides a different approach to summarising the results with the most up-to-date and comprehensive review of the literature.

In this work, we would like to summarise various results achieved in cyber insurance so far and outline further directions for the development. Our study has the primary focus on scientific achievements, but we also provide a bit of the practical insights for the most up-to-date comprehensive picture. Thus, we provide a brief history, outline the current practices and sketch future predictions, for the cyber insurance market (see Section 3). The survey summarises the background information on cyber insurance, in order to introduce readers into the basic terms, process and mathematical models on the topic (see Section 2). We do not have a goal to provide a comprehensive tutorial on cyber insurance, but help to understand the core concepts, which are usually only briefly mentioned in the dedicated articles. Next, we discuss the peculiarities of cyber insurance, as one of many applications of insurance (See Section 4). We underline the main issues which have to be taken into account when cyber risks are insured. The core analysis of the available approaches is performed in Section 5.1. We collected various practices available for risk assessment process and showed how they can be applied in the cyber insurance process. Further-

more, we analysed scientific approaches to cyber insurance, taking into account various initial assumptions and problems studied (Section 5.2). To our knowledge, this is the first attempt to summarise the dispersed results under the same umbrella. Section 6 concludes the paper with possible further steps to overcome the existing problems of cyber insurance.

2 Basics of insurance

This section is devoted to the definition of basic concepts of insurance. These concepts are relevant for all insurance markets, including cyber insurance. We intentionally single out the basic concepts to underline the main features specific for cyber insurance outlined in Section 4.

2.1 Basic Definitions

In this section we define the main terms used in insurance. We start with the description of the main actors. Then, we define the core concepts of risk management. Although, insurance is just one type of risk treatment, its correct and reliable operation heavily depends on some steps of risk management. Finally, we provide definitions of the main terms of insurance contract establishment and claim handling.

Actors We start with the definition of the main actors. *Insurer (insurance carrier)* is a party that assumes risks of another party in exchange for payment. *Insured (policyholder)* is a party that asks for insurance and would like to transfer its risk. From the market point of view, the insurer is considered as a supply side, when the insured is a demand side. In this paper we use also a term *agent* to refer to a party that potentially can buy an insurance, but it is irrelevant for the consideration whether it actually has already bought the insurance or has not. The insurance process also may involve other parties like a *verifier*, a *consultancy agencies*, *police*, etc, which roles are self-explanatory.

Risk management Insurance is a way to manage risks. Moreover, the idea of risk management has been originated and generalised from insurance management [144]. Thus, in order to understand the insurance we should define the risk management first.

Risk is the possibility of suffering harm or loss [5]. First, this definition underlines that risk is not a certainty, but a possibility of risk occurrence in the future. A risk occurrence is called an *accident*. This possibility of risk occurrence depends on two aspects: threat and vulnerability. *Threat* specifies the cause of risk (fire, kidnapping, leakage of confidential information, etc.). *Vulnerability* is an existing flaw or weakness which can be exploited and result in an accident.

Second, the definition of risk states that risk may result in losses for an agent. Losses occur because of the consequences of an accidents, called *impact*.

Impact may be tangible (e.g., loss of revenue or financial penalties) or intangible (loss of productivity or loss of reputation), depending on the impacted assets. By *assets* we mean anything valuable for the organisation. An asset can be a physical object, but also secrete information, a business goal [145], etc.

Thus, a risk exists only when there is a cause, a possibility and consequences of an accident. In other words, risk is a combination of a threat, a vulnerability and an impact.

Risk management is a process of identifying risks and implementing plans to address them [5]. The essential parts of the risk management process are risk assessment and risk treatment. *Risk assessment* is a subprocess of risk management consisting of risk identification and risk analysis. First, *risk identification* lists and characterises elements of risk: threats, vulnerabilities and impact. Then, risk is estimated with *risk analysis*. Risk analysis is performed with two risk parameters: the probability of an accident and the amount of impact of the accident, and can be seen as:

$$Risk = Probability \times Impact \tag{1}$$

Risk analysis can be *quantitative* or *qualitative*, depending on whether real values or abstract levels are used.

Risk treatment is a sub-process for selection and implementation of measures to deal with the significant risks. There are four possibilities to deal with risk: risk mitigation (or risk reduction), risk transfer, risk avoidance, and risk acceptance. *Risk mitigation* are actions helping to reduce risk (i.e., reduce the probability of a risky event occurrence, its impact or both). *Risk transfer* is sharing the burden of potential losses with another party. Insurance is one possibility for risk transfer. *Risk avoidance* is a decision to avoid the risky event (e.g., withdraw from the risky part of business). *Risk acceptance* is simple acknowledgement that the estimated losses may take place. Naturally, risk acceptance is automatically applied even without any decision explicitly taken.

Insurance contract. *Insurance policy* is a contract between an insured and an insurer which defines terms, conditions, and exclusions for the insured risk. *Premium* is a fee paid by the insured to the insurer for assuming the risk. *Exclusions* are the risks excluded from an insured policy. *Coverage* is the amount of risk or liability covered by insurer. There are two types of insured coverages: *first-party* and *third-party*. The difference between these two types of coverages is in the parties covered: the *first-party* coverage insure against the losses for the insured itself, when the *third-party* coverage covers the damage to third parties. An example could be a fire insurance policy, which, in case of an accident, refunds the losses caused by the damage to the building to the insured (first-party coverage) and covers the expenses for the injured people (third-party coverage).

When an accident occurs, the insured activates the insurance policy by sending a *claim* to an insurer. In this case the insurer covers partly (partial insurance) or completely (full insurance) the losses of the insured. This payment is

called *indemnity*. A part of losses still carried by insured is called *deducible*. Losses of an event occurred may be primary or secondary. Primary losses are direct consequences, when secondary losses are indirect. Examples of secondary losses are losses to the reputation or decrease in stock market.

2.2 Basic Insurance Formalisation

This subsection introduces the basics of the mathematical model for cyber insurance. The model is based on the utility function, which can be seen as the amount of satisfaction for an agent when a certain amount of wealth is in its possession. Such approach allows differentiating the real expected wealth and is perception (including feeling of risk) for agents.

2.2.1 Demand Side. Insured

Utility function Let W denote the wealth of an agent and W^0 be its initial wealth. Let also an accident happens with the probability **pr** and causes losses L. Thus, in case of an accident the resulting wealth of the organisation is $W = W^0 - L$, when in case of no accident the wealth is still $W = W^0$. Nevertheless, it is assumed that an agent does not consider pure wealth but a utility of the wealth. Let $U(W)$ be a function, which returns the utility of the wealth W. Then, the expected utility for the agent in case of no insurance option available/taken can be seen as:

$$E[U(W)] = (1 - \mathbf{pr}) \times U(W^0) + \mathbf{pr} \times U(W^0 - L) \tag{2}$$

The exact form of the utility function also depends on the attitude of an agent to risk, which could be either risk averse, risk neutral, or risk seeking. In case of several alternatives with the same average outcome, a *risk averse* agent prefers the alternative with less risk, a *risk seeking* agent - with most risk and a *risk neutral* agent has no preferences. Insurance requires agents to be risk averse. This means, that the expected utility function is a von Neumann-Morgenstern utility of wealth function, which is assumed to be twice deferential and concave: $U'(W) > 0$ and $U''(W) < 0$.

Utility function with insurance. If an organisation buys insurance it pays a premium P and gets an indemnity I in case of an accident. Insurance policy, proposed by an insurer, is then can be seen as a tuple: (P, I). Thus, the overall wealth in case of insurance and an accident is $W = W^0 - L - P + I$, when without an accident the wealth is $W = W^0 - P$. The expected utility in this case is:

$$E[U(W)] = (1 - \mathbf{pr}) \times U(W^0 - P) + \mathbf{pr} \times U(W^0 - L - P + I) \tag{3}$$

Self-protection. An agent may invest in self-protection to reduce the exposure to the risk. This investment increases the security level and decreases the final wealth of the agent. Let x be a protection level and $C(x)$ be a function which returns the cost of the investments to reach level x. $C(x)$ is a twice deferential function which is assumed to be strictly convex: $C'(x) > 0$ and $C''(x) > 0$. In other words, the effectiveness of investments in protection decreases with the increase of the protection level x.

Naturally, **pr** also depends on x. Moreover, in a more general situation this function also depends on the protection level of other agents (e.g., a virus may attack a system through a trusted channel established with a partner which has been recently compromised by this virus). This effect of protection level of one agent on another agent is called *externalities*. Externalities could be *positive*, when the probability of an accident for one agent decreases because of increase of the protection level of another agent, or *negative* otherwise. Note, that dishonest agents may avoid investments in self-protection, enjoying the effect of positive externalities. This problem is known as a *free riding problem*.

Let X be a vector of protection levels of all agents in the system. If we consider an agent i with x_i, then the security levels of all agents except the agent i can be denoted as X_{-i}. Thus, from now on we change **pr** to a function $\mathbf{pr}_i(x_i, X_{-i})$ returning the probability of an agent i to be compromised (both directly or indirectly). We refer to this function as an *accident probability function*. Naturally, if the agent may be attacked only directly, then $\mathbf{pr}_i(x_i, X_{-i}) = \mathbf{pr}_i(x_i)$, and is denoted as: $\pi_i(x_i)$. The accident probability function is also twice deferential and convex ($\frac{\partial \mathbf{pr}_i}{\partial x_i} < 0$ and $\frac{\partial^2 \mathbf{pr}_i}{\partial x_i^2} \geq 0$)[1].

Now we can rewrite the expected utility $E[U_i(W_i)]$:

$$\begin{aligned} &\textit{with insurance}: \\ &E[U_i(W_i)] = (1 - \mathbf{pr}_i(x_i, X_{-i})) \times U_i(W_i^0 - P_i - C_i(x_i)) + \\ &\qquad \mathbf{pr}_i(x_i, X_{-i}) \times U_i(W_i^0 - L_i - P_i + I_i - C_i(x_i)) \end{aligned} \tag{4}$$

$$\begin{aligned} &\textit{without insurance}: \\ &E[U_i(W_i)] = (1 - \mathbf{pr}_i(x_i,))X_{-i}) \times U_i(W_i^0 - C_i(x_i)) + \\ &\qquad \mathbf{pr}_i(x_i, X_{-i}) \times U_i(W_i^0 - L_i - C_i(x_i)) \end{aligned} \tag{5}$$

If $L_i = I_i$ the insurance is *full*, i.e., completely covers the losses when the threat occurs. The insurance is called *partial* when $L_i > I_i$. The partial insurance can be modelled as: $I_i = \beta_i(L_i - D_i)$, where β_i is a portion of losses the insured i wants to be covered by and D is a deducible. Now, we can use only Equation 4, since Equation 5 can be derived from Equation 4 when the selected contract is (0;0). This contract can be received if $\beta_i = 0$, since a premium is usually proportional to an indemnity (i.e., $P_i = 0$ when $I_i = 0$).

Agents modify theirs security levels and choose the available insurance contracts (either selecting from a set of the proposed contracts or specifying the

[1]Note that in this case we have partial derivatives, since $\mathbf{pr}_i$ depends on a number of $x_j \in X$.

portion of losses to be covered) in order to maximise theirs expected utility (i.e., Equation 4).

Agents may be considered as *homogeneous* or *heterogeneous*. The insureds are considered as homogeneous if all invariable parameters are identical, i.e., $W_i = W_j$ and $L_i = L_j$, and all functions are identical: $\forall i, j \quad E[U_i(W)] = E[U_j(W)],\ C_i(x)) = C_j(x),\ \pi_i(x) = \pi_j(x)$. The agents are heterogeneous if these functions and parameters (or at least some of them) are different. Note, that in some cases environment and network topology may cause different impact on different agents [148].

Social welfare. So far we considered the problem form a perspective of a single agent. This perspective is useful for description of a selfish behaviour of an insured. The regulatory entity (e.g., a government) may be interested in the overall impact of cyber insurance on the society in general, i.e., *social welfare*. Mathematically, the social welfare model usually applied in insurance can be computed as the sum of all expected utilities:

$$SW = \sum_{\forall i} E[U_i(W_i)] \tag{6}$$

The natural goal of this regulatory entity is to maximise the Equation 6.

2.2.2 Supply Side. Insurer

Profit of insurer. The insurer can also be considered as risk averse, but since most papers on the studied topic consider it as risk neutral, we also stick to this assumption. Thus, the overall profit and utility of an insurer can be computed as:

$$U(W_s) = W_s = \sum_{\forall i} (P_i - \mathbf{pr}_i(x_i, X_{-i}) \times I_i) \tag{7}$$

Market types. The pricing strategy (e.g., the specification of (P_i, I_i)) for an insurer is determined by the type of the market in consideration. Three types of market usually can be found in the literature:

- *Competitive*. This is the most common type of the market model. In this model it is assumed that the pool of insurers is infinitely large and none of the existing or incoming insurers is able to propose a contract better than the existing ones. From the mathematical perspective this means that the premiums charged by insurers are *fair premiums*, i.e., $P_i = \mathbf{pr}_i(x_i, X_{-i}) \times I_i$. In this case, according to the Equation 7 the insurer has zero profit.

- *Monopolistic*. When an insurer is considered to be monopolistic it is free to specify any premium for a contract. On the other hand, too high premiums may result in a low number of buyers. Thus, the most natural condition

in the monopolistic market is maximization of profit (e.g., Equation 7). Another important case of monopolistic market is when the monopolistic insurer is considered mostly as a regulator, rather than a greedy participant of the market. In this case the insurer gets no profit and often serves more like a re-distributor of funds depending on the security levels of agents (e.g., Equation 7 is zero).

- *Immature/Oligapoly.* When the insurance market is immature, i.e., a number of available insurers is too low for the market needs, then the insurers can define the premiums higher than the fair premium: $P_i = (1 + \lambda)\mathbf{pr}_i(x_i, X_{-i}) \times I_i$. This *loading* of λ can be explained as: administrative costs, additional profit, safety capital (the amount of money required by the insurer to avoid probabilistic fluctuations of claims), etc.

Here we have to underline that estimations of premiums also can be performed using other mechanisms, not depending on the market [93]. On the other hand, all papers on cyber insurance analysed in this survey consider one of the three specified ways to set up the price (depending on the market type under consideration).

Life vs. non-life insurance. The difference between the life and non-life insurance is self-evident. Roughly speaking, life insurance has its primary focus on insuring the agents against their death, when non-life insurance is mostly relates to any other type of insurance (also called causality insurance). Consequently, life insurance assumes that an accident for one insured occurs only once. The accidents covered by a non-life insurance may occur several times in a considered period. A typical period of non-life insurance is one year [7, 93, 124]. Thus, in case of life insurance, it is enough to consider only the probability of occurrence (e.g., $\mathbf{pr}_i$), when for non-life insurance it is required to find a rate of occurrences RO_i, i.e., a number of accident occurrences in a considered period of time t. Although, cyber-insurance is clearly a non-life insurance the available state of the art literature on the topic considers only a single event in an observed period (i.e., using $\mathbf{pr}_i$ instead of RO_i). Instead, for complete non-life insurance fair premium estimation the following formula should be used: $P_i = RO_i(t)I_i$ [93].

Naturally, RO_i is a random variable by itself and can be modelled with a specific process (e.g., Poisson process or renewal process [93]). Although, analysis of its distribution is desirable, the accurate definition of the distribution is often very problematic. A more common approach is to assess the mean value of risk derived from the expected value of RO_i. The expected value of RO_i is derived from practical, statistical observations (the average value is assumed to be equal to the expected value of RO_i). The later observation underlines the practical importance of availability of genuine, complete, and representative statistical data for correct assessment.

Simple game. Now it is possible to specify mathematically the behaviour of the agents and the insurer.

First, the invariable values are specified[2]: W_i, L_i and D_i. The insurer specifies the contract it is ready to offer. Here we would like to distinguish between two actions of an insurer. By specification of a contract we mean the definition of *rules* for computation of premium and indemnity. By instantiation of a contract we mean the computation of the values (premium and indemnity) when all required parameters (usually, protection levels x) are available.

The most important action allowed for an insured is the *selection of the desired level of protection* x_i (or level of investments, if security is considered as a function of cost $x_i(C_i)$). Also, the agent is allowed to *select the contract* (i.e., apply for the contract specified by the insurer and specifying the portion of the losses to be covered).

In this simple case, the (cooperative) game has the following 2 phases:

1. Agents specify their protection level and select the available contract type to maximize their Equation 4.

2. The insurer specifies the selected contract for agents, e.g., (premium, coverage), using the protection level of the agents. The pricing policy of the insurer is driven by the considered market (e.g., maximise Equation 7 for a gready monopolistic insurer or using a fair premium for competitive market).

2.2.3 Information Asymmetry

Adverse selection and moral hazard. The situation when some information is available to some participants and is not available to others is called *information asymmetry*. In general, all participants may suffer from the information asymmetry [15, 16], but there are two cases which received a special attention.

- *adverse selection* is a situation when an insured with higher risk exposure wants (or continue) to buy an insurance more than the insured with lower exposure. Such situation is possible when the insurer does not have information about the probability of an event for agents or does not discriminates agents according to their protection level. Therefore, the insurer cannot distinguish between agents with high and low risks *before signing a contract*.

- *moral hazard* is a situation when an insured behaves in a riskier way than usually. Such situation is possible when the insurer does not have enough information about the actual behaviour of the insured. Therefore, the parameters, which were used for defining premium and indemnity, may change *after signing the contract*.

[2]Some of these values also may vary, but it is not a primary focus for the majority of researchers.

The insurer in both cases is not able to compute premiums using the real probability of accident occurrence, but it is often assumed to know the distribution of the possible probabilities among agents.

The game with adverse selection. The first problem is modelled by separating all agents into two profiles: low and high risks, where all agents in a profile have the same security level. The usual solution for this problem is *separation* of contracts for agents from different profiles [123]. Two contracts are proposed to agents, where each contract is profitable for agents from one group only. From a theoretical point of view, in most cases, one contract may propose full insurance with high premium (for high risk users), when the second one provides only a partial coverage but for a much smaller price.

When the adverse selection problem is modelled the *agents start with their protection levels specified and are not able to change them.* Then:

1. The insurer specifies a set of contract(s), e.g., (premium, coverage), using the general knowledge (e.g., distribution of probabilities of threat occurrence).
2. Agents select one of the proposed contract.

The game with moral hazard. In case of the moral hazard problem agents are free to choose a security level, when the insurer does not know which level each agent will have after signing the contract. The usual solutions to moral hazard problem are *deducibles/partial coverage* and *observations* by insurer [132, 13].

When moral hazard problem is modelled the game is as follows:

1. The insurer specifies contract(s), e.g., (premium, coverage), using the general knowledge (e.g., distribution of probabilities of event occurrence).
2. Agents select the contract and specify their security levels/investments.

2.2.4 Organizational Environment

Market regulation options. There are several ways for regulators to govern the insurance market. We have found the following regulatory techniques in the literature:

- *Mandatory insurance.* In some cases insurance can be mandatory. In this case the agents cannot choose the option "proceed without insurance", or buy 0 indemnity, even if this option has higher utility for agents.
- *Fines and rebates.* In addition to premium discrimination based on the probability of accident occurrence, the model may enforce additional fines (rebates) for agents with low (correspondingly, high) protection levels.
- *Mandatory investments.* Some models require a minimal level of protection investments.

2.3 Insurance Process

Phase 0: Self-Assessment and Treatment by and Agent. Initially, before engaging in cyber insurance, an agent performs self-assessment and decides which risk it would like to transfer and whether the transfer option is more efficient rather than others. This is an important phase, which does not yet belong to the insurance process itself. Therefore, we mark this phase as Phase 0. First, the agent identifies the main parameters of risk: valuable assets, possible threats and existing vulnerabilities in the security system. Then risk is analysed by determining the likelihood and possible impact of an accident. Finally, these values are aggregated to get risk values. Finally, the agent prioritises risk according to some defined criteria, identifies possible treatments, prioritises them and implements those, which have been selected. One of the possible treatments is risk transfer, which usually means insurance against the risk.

1. Risk Identification
   (a) Asset Identification.
   (b) Threat Identification.
   (c) Security/Vulnerability Identification.
2. Risk Analysis
   (a) Likelihood Determination.
   (b) Impact Determination.
   (c) Risk Estimation.
3. Risk Treatment.
   (a) Risk Prioritization
   (b) Identification of Treatments
   (c) Prioritisation of Treatments
   (d) Implementation of Treatments

Phase 1: Issue Insurance Policy to an Agent. When an agent decides to buy an insurance policy, it is now an insurer which needs to estimate the risk of the agent. Therefore, steps for the first two sub-phases of Phases 0 and 1 are the same. The key difference for these two sub-phases are: 1) the executive entity (agent in Phase 0 and insurer[3] in Phase 1) and 2) the information available to these entities (in Phase 1 less information about the system is to be revealed to the analysts). Naturally, re-usege of the assessment results is possible, but the insurer has to be assured that the results of self-assessment are correct. The insurer needs the risk assessment of the agent in order to specify the contract. The insurance contract restricts the considered threats, indemnity limit and states the premium price, which is estimated using the risk values. Finally, the contract is properly written and signed.

[3]Or a verifier acting on behalf of the insurer.

1. Risk Identification
    (a) Asset Identification
    (b) Threat Identification
    (c) Security/Vulnerabilities Identification
2. Risk Analysis
    (a) Likelihood Determination
    (b) Impact Determination
    (c) Risk Estimation
3. Establish Contract
    (a) Coverage Specification
    (b) Premium Estimation
    (c) Write and Sign Contract

Phase 2: Claim Handling. Claim handling phase is initiated when (if) an accident takes place. First the insured notifies the insurer about the accident. Often, the insured has to notify the law enforcement agencies before this step. The insurer considers the claim and collects the evidence about the accident. In the meanwhile the insured computes losses, collects the required information and submits the claim. The insurer checks the assumptions of the contract and accident evidences. In case of a conflict between an insured and an insurer the case is resolved in a court. Finally, the claim handling sub-phase overs with loss coverage (if the case is proved to be within the conditions of the contract).

1. Accident Notification
2. Evidence Gathering
3. Loss Computation
4. Claim Submission
5. Contract Assumptions check
6. Resolve the Conflicts
7. Losses Coverage

Phase 3: Policy Renewal. When the contract is over and the partners may be willing to renew it. The process itself is very similar to the one for phase 1, but some steps may be relaxed, much information can be re-used, and the statistical data, collected by the insurer during the previous period, updated.

1. Risk Re-Identification
   (a) Asset Re-Specification
   (b) Security control Re-Identification
   (c) Vulnerability Re-Identification
2. Risk Re-analysis
   (a) Likelihood Re-Determination
   (b) Impact Re-Determination
   (c) Risk Re-Estimation
3. Re-Establish contract
   (a) Coverage Re-Specification
   (b) Premium Re-Estimation
   (c) Re-Write policy
   (d) Re-Sign policy

2.3.1 Insurability Criteria

Several authors proposed the conditions for verifying whether a specific risk can be insurable. The more a specific risk satisfies these conditions the more precise the predictions are about this risk, and the more reliable the insurance process is.

Insurability criteria by Mehr and Cammack. R. Mehr and E. Cammack [91] formulated seven requisites of insurable risk:

Accidental loss. The accident must be fortuitous and not under control of insured.

Limited risk of catastrophically large losses. Catastrophically large losses must happen with very low frequency.

Calculable loss. It must be possible to estimate or calculate possible losses and probability of an accident.

Large number of similar exposure units. A large number of homogeneous exposure units must be available to facilitate the probability determination.

Affordable premium. The premium must be reasonable with respect to the insured.

Definite loss. The loss must be difficult to forge. Its time, place and cause must be easy to determine.

Large loss. The losses must be large enough for the insured to be born by himself/herself.

Insurability criteria by Berliner. R. Berliner [20, 24] formulated nine criteria of insurable risk (the first five criteria refer to actuarial-mathematical model, sixth and seventh to the market conditions, and the last two to environment):

Randomness of loss occurrence. Accidents must happen independently.

Maximum possible loss per accident should be manageable for insurer.

Average loss per accident should be moderate.

Loss exposure should be large enough.

Information Asymmetry should be too high.

Insurance premium should be affordable for the insureds.

Cover limits should be suitable for insureds.

Public limits should be respected.

Legal restrictions should not be violated.

3 Market Solutions for Cyber-Insurance

In this section we describe the state of practice, i.e., insight into the cyber insurance business reality. First, we provide some historical remarks on the development of the cyber insurance market, then we sketch the current practice and finish the section with the predictions made by leading cyber insurers and analysts.

3.1 Past of cyber insurance market

Specialized coverage against computer crime first appeared in the late 1970s [88]. In 1990, insurance policies started to be offered by security software companies partnering with insurance companies as packages (software + insurance) [85]. In 1998, the earliest known separate hacker insurance policies were first introduced by ICSA Inc., the International Computer Security Association. This organization offered insurance against hacker attacks as a part of its TruSecure service [118, 77, 88].

Over the years, cyber insurance policies have become more and more sophisticated in order to be in line with the continuous evolution of cyber attacks and the complexity of information systems. So their sales began to rise because of the severe cyber events occurring within major companies that caused big losses. In February 2000, online hackers launched what's known as a "denial of service" attack, shutting down eBay, Amazon.com, CNN.com and other major Web sites for as long as three hours. By some estimates, the event costed the companies $1.2 billion [54]. Companies that experienced these disasters became much more interested in purchasing cyber insurance policies to mitigate future losses [119]. Successively, companies like Counterpane Internet Security started offering cyber security insurance. In 2000, the same company announced [59] that its clients could purchase up to $100 million in insurance coverage to protect against loss of revenue and information assets caused by Internet and e-commerce security breaches.

In 2003, amount of introduced cyber insurance policies grew significantly in US [61]. In fact, in that year California passed the data breach notification law [138] that required a state agency, or a person or business that conducts business in California to disclose any data breach. The Californian law has been a model for legislation passed in over 30 US state legislatures and there are moves to implement a national notification standard concerning compromised data [10]. Since then many countries started considering the possibility to introduce similar laws. There have been moves at the federal level in Canada to introduce a data breach notification law [10], although currently only the province of Ontario requires the notification after a security breach. In 2007, an Australian senator put forward a Private Members Bill amending the Privacy Act to require agencies and organizations to report data breaches [10]. In January 2012, the European Commission unveiled its draft data protection Regulation (Regulation), intended to update and harmonize EU data protection law [116, 64]. According to the European Parliament legislative resolution of 12 March 2014 on the proposal, as soon as the controller becomes aware that a data breach has occurred, the controller should notify the breach to the supervisory authority within 24 hours (it has been changed to 72 hours after the first reading [116]).

3.2 Current cyber insurance market status

Security coverage. In a survey conducted by ACE in 2012 [90], 99% respondents replied that they suffered from IT or cyber loss, 27% of respondents rated cyber attacks as a key risk, and 30% placed media and reputation damage as the highest cause of internal concern. To these expectations insurer carriers replied with a large number of cyber insurance policies.

Our analysis of current cyber insurance policies available on the market (see Table 1) shows that common first-party coverage includes loss or damage to digital assets, business interruption, cyber extortion, theft of money and digital assets. Common third-party coverage may include security and privacy breaches costs, computer forensics investigation, customer notification costs, multi-media liability, loss of third-party data, third-party contractual indemnification. The

	Coverage	*Allianz*	*QBE*	*AEGIS*	*CNA*	*InsureTrust*	*CDRM LLC*	*Travelers*	*Zurich*	*ACE*	*Hiscox*	*Insureon*	*Marsh*	*Chubb*	*AIG*
First-Party	Loss or damage to digital assets	×*	×	×	×	×		×	×	×	×	×	×	×	×
	Business Interruption	×*	×	×	×*	×	×	×	×	×	×	×	×	×	×
	Cyber extortion	×	×	×	×*	×	×	×	×			×	×		×
	Theft of money and digital assets	×	×		×*		×	×	×	×	×	×	×	×	
Third-Party	Security and privacy breaches	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	Computer Foresincs Investigation	×	×	×*	×	×	×			×		×			×
	Customer notification/PR expenses	×	×		×	×	×	×	×	×		×		×	×
	Multi-media liability	×	×	×		×		×	×*	×					×
	Loss of third-party data	×*		×	×*	×	×	×	×	×	×	×	×	×	
	Third-party contractual indemnification		×			×			×	×				×	

Table 1: Coverage of several existing insurance policies.

available indemnity ranges from 10 millions up to 200 millions depending on the selected packages [6].

Additionally, some policies next to the damage coverage, offer prompt support in case of a loss, or other cyber events through the assistance of specialized cyber specialists, often connected to a crisis management service to identify the problem as quickly as possible and to ensure its prompt resolution (e.g., QBE [122]).

Privacy coverage. Particular attention is given to privacy. Privacy coverage is clearly driving the market [22]. For example, the company ACE has a specific product called ACE Privacy Protection® [1] which provides specific coverage up to $20 million and focuses on privacy liability.

Cyber insurance domains. According to the 2014 Batterley Risk Report [22], now market trends seem to increase, especially in health care and the small- to mid-sized insureds segments. For example, Chubb is already providing a product called Cyber Security for Health care Organizations that offers coverage for cyber risks related to the medical field [40]. According to a study of actual claim payouts in 2013 [58], PII (personally identifiable information) and PHI (private health information) were the most commonly exposed data. In this study, the number of claims submitted for these two data types was almost identical, 40 for PII (28.7% of claims) and 38 for PHI (27.1%). In fact, out of 145 data breach insurance claims analyzed in this report, the healthcare was the sector most frequently breached (29.3%). Other market sectors interested in cyber insurance are the retail sector, financial services, professional services, utilities sectors, etc. [3].

Agent attitude to cyber insurance. Some companies are still not convinced that investing in cyber insurance is the way to go. According to the survey of Enterprise-Wide Cyber Risk Management Practices in Europe conducted by Advisen in 2015 [34], the majority of respondents said that they do not purchase cyber insurance because insurance does not provide adequate coverage for their exposures (47%). The second and third popular answers were:

it is too expensive (20%) and adequate limits are not available in the market (7%). These results coincide with the findings of Batterley Risk Research [21]; existing insureds reported that they would be willing to pay higher premiums if their primary coverage objectives were included in the cyber policy. Although some companies are still hesitant about buying policies due to many exclusions, restrictions and uninsurable risks, those that adopted the insurance policies declared to be satisfied [119].

3.3 Future of the cyber insurance market

USA. Despite optimistic promises, the market is still below the expectations. Even a conservative forecast of 2002, which predicted a global market for cyber-insurance worth $2.5 billion in 2005, turned out to be five times higher than the size of the market in 2008 (three years later) [79, 28]. Although the market does not develop as quickly as it was predicted, it still has a room for growth and becomes larger and larger with every year. The Betterley Risk research conducted in 2014 [22] revealed, that the current gross premiums for cyber-insurance in US is 2.0 billions (and was 1.3 billion, in 2013) growing 10-25% per year, that coincides with the predictions of Marsh & McLennan Co [76]. The most recent report [23] has shown that the annual gross written premium could be around 2,75 billions in 2015.

Europe. In Europe, the cyber insurance market is slowly growing as well. As reported by the Fourth Annual Survey of Enterprise-Wide Cyber Risk Management Practices in Europe conducted by Advisen [34], while the European cyber insurance market is still significantly below the levels seen in the U.S., (the European market is estimated to be less than $150 million) it is rising by 50% to 100% annually, according to Marsh [76]. Thus, the cyber insurance market in Europe is a great opportunity with potential and low competition.

4 Cyber-Insurance

This section is devoted to the key peculiarities of cyber insurance with respect to insurance in general. We first list these peculiarities found in the literature. Then, we focus on the models for protection level interdependencies. Strictly speaking, interdependency of protection levels does not relate to cyber insurance only, but it is one of the most affected area of insurance application. Finally, we finish the section with the insurability analysis of cyber insurance to show whether insurance is applicable to cyber risks.

4.1 Peculiarities of Cyber-Insurance

Here we summarise the main issues with applying insurance to cyber security. We group the issues by phases and steps of our methodology. We do not consider the Phase 0, since: 1) it is optional for the cyber insurance process; 2) because

we consider risk management only in scope of the main topic of the survey, i.e., cyber-insurance; 3) because most of these steps also belong to the steps of Phase 1. Moreover, since Phase 1 has got more attention in the literature and by practitioners we break the relevant issues by sub-phases and steps.

4.1.1 Issue insurance policy to an actor. Risk Identification.

Insurers lack of experience and standards. Cyber insurance is a novel type of insurance and insurers do not yet have standardised procedures for dealing with it [11, 38, 142, 88, 22].

Evolution of system. Computer systems evolve fast. First, the system of an organisation may easily change. Second, new technologies (e.g., cloud) appear very often, changing the landscape of cyber risks [47, 124, 99].

4.1.2 Issue insurance policy to an actor. Risk analysis. Likelihood Determination.

Information Asymmetry. Insurance works poorly in presence of high information asymmetry, i.e., the situations when both an insured and an insurer do not have access to the same information [94, 47, 142, 24, 56, 60, 99, 13]. In the cyber world, this issue, common for many insurance markets, is especially important. There are many obstacles for an insurer to get the reliable information about the risk exposure of an insured, and even more obstacles to know that this exposure will be maintained at the specified level during the whole period of policy operation. Some chief security officers do not want to reveal the applied methods to external parties and be forced to install additional controls [100]. Furthermore, it is easy to install protective software (e.g., a firewall, antivirus) and poorly maintain them properly [11]. Finally, insurers should not forget that security is a process, not a product [128, 16, 124].

Hard to specify rate of occurrences - computation of risk exposure is based on the rate of occurrences parameter, which is extremely hard to specify for cyber risks [62, 124]. Although the determination of rates of occurrences itself is a hard task (see, for example, papers on security evaluation, like [75, 80]), several reasons make it even harder:

Evolution of attacks - techniques used by attackers are constantly changing. New attacks come to play, when old ones vanish. The attackers are highly adaptable and changes are very unpredictable [24, 149, 9, 22].

Effectiveness of measures and standards - it is unclear how exactly security measures and standards affect the actual level of security/risk of the organisation. Thus, it is difficult for insurance to define the requirements for reducing premiums [47, 142, 14, 45].

Interdependence of security. Security level of one system (may) depends on security of others: a virus may penetrate into the system through the channel established with a partner (with much weaker security) [47, 142, 24, 28, 88, 12, 128]. This makes investing in your security much less effective and leads to the free-riding problem.

Lack of statistical data. Absence of statistical data on incidents does not allow insurers to specify their policies reliably [90, 47, 142, 24, 56, 131, 88, 60, 99]. The information on cyber threat accidents is often kept private preventing spreading of knowledge and making the following problem more important for security:

Information sharing barriers - companies often do not want to reveal breaches, since it will cause larger (often, non covered) secondary damage than the direct impact, e.g., to reputation [90, 11, 60, 101, 99]. There is no publicly available comprehensive and consistent database of breaches [94]. For example, Biener et al. [24] analysed SAS OpRisk Global Data, the largest collection of publicly reported operational losses, but this database contained only about 1000 cyber-related reports of world-wide losses occurred between March 1971 and September 2009. It is necessary to share information between insurers and insureds [13].

4.1.3 Issue insurance policy to an actor. Risk analysis. Impact Determination.

Hard to estimate damage. Quantifying the impact of a cyber attack is a fundamental factor for insurance since cyber crimes or data breaches may lead to many business repercussions [47, 142, 56, 87, 60, 101, 99]. Moreover, damage may be very hard to quantify in advance for cyber risks because of the nature of information assets (e.g., know-how cost, or private identifiable/health information). Also, reputation cost, which accounts for large portion of the whole damage is very difficult to estimate.

4.1.4 Issue insurance policy to an actor. Risk analysis. Risk Estimation.

Hard to verify. It is currently almost impossible to verify correctness of the estimated risks [75].

4.1.5 Issue insurance policy to an actor. Contract Specification. Coverage Specification.

Unclear coverage. It is hard to specify what an insured wants to be covered from and an insurer is willing to cover precisely [47, 24, 46, 45]. This issue is particularly hard with the dynamicity of threats.

Exclusions and limited coverage. Current policies contain a lot of exclusions [11, 119] and are limited in coverage [142, 119, 21, 128, 22, 99].

Low Indemnity limits. The indemnity limits are too small (max 200 millions) for large corporations, like Google.

4.1.6 Issue insurance policy to an actor. Establish contract. Premium Estimation.

Correlated risks. Risk threatening one insured may also correlate with risk for another insured. Examples: worms, similar bugs, etc [94, 47, 142, 22, 99]. On the other hand, Biener et al., [24] showed that only about 17% of reported threats affect more than 1 organisation. Moreover, correlation of risks is particularly dangerous for cyber world because of:

Lack of re-insurance - insurers themselves bare risks. They would like to re-insure the highest risks (e.g., for large epidemics) to higher level insurers [47, 142, 24, 11, 28]. Although currently there is not much re-insurers available there is a tendency for such actors to become more and more interested in cyber risks [23].

Geographical similarity - there is almost no difference between computer systems in different geographical regions, making the geographical risk diversification solution much less attractive. This means that attackers (e.g., worms) can be as effective with their attacks in China as they are in US. Biener et al., [24] showed that there is the difference between the number of reported incidents across the World in absolute numbers. On the other hand, such difference can be explained by the fact that more developed countries depend more on IT, i.e., they are more exposed to attacks.

Monoculture - many systems are alike, e.g., many systems use Windows operational system and have the same vulnerabilities [28, 53, 14, 22].

Easy to perform - Attacks are easy and cheep to perform. The adversary may attack from any place in the world. Moreover, it is extremely hard to track them down, e.g., to punish. Many organisations do not even notify police about the breaches [56, 125]. Moreover, it is easy to replicate an attack and launch it against a large variety of systems simultaneously (e.g., worms, botnets).

4.1.7 Issue insurance policy to an actor. Establish contract. Write and Sign Contract

Language The contractual language for cyber insurance is still vague and imprecise. It is hard to define precisely what is covered and what is not [147, 11, 22].

Overlapping with existing insurance coverage. Companies think that they don't need cyber insurance since their general insurance package already covers their needs [47, 9, 99, 124].

Liability. When a cyber attack or incident occurs it is necessary to establish the levels of responsibility for the damages and define who is responsible for the losses. In the digital world this is not always clear [142, 11, 53, 94, 14, 125, 45, 9, 99]. In some cases these are the system owners, but in others these could be software producers, ISPs, etc. This issue is especially troublesome with the cloud technology [99].

4.1.8 Claim handling.

Time for claims. Many attacks occur undetected. The breach may be noticed long after the attack. Furthermore, some attacks are extremely lengthy (e.g., attacks may take months). It is not clear how insurers should reimburse the expenses.

Forensics. The insurers often require proper investigation of accidents before making a claim. This imposes additional burden on the insured and hurts the reputation of the company, since the organisation is no longer able to keep the accident confidential. These secondary losses, often not covered by an insurer, may prevent the agent from notifying the law enforcement agency and making a claim [15, 14].

4.1.9 Policy renewal

Since this phase is simply re-consideration of a contract all problems relevant for *Issue insurance policy to an actor* phase are relevant for this phase as well.

4.2 Cyber-Insurance Formalisation

Simple interactions between an isolated insured and an insurer usually may be described with classical models for insurance, and are not very specific for cyber-insurance. Therefore, the majority of authors consider a more complex situation, when many (sometimes very large amount of [130]) insureds are connected by a network. The network can be a usual IT network, or some other way of agents connections (e.g., social network).

Security threats are often correlated and can exploit the network to infect other nodes. Thus, the overall security of an agent depends not only on its own security level, but also on the security levels of all adjacent nodes. Thus, the security levels of agents are *interdependent*.

Let $\pi_i(x_i)$ be the probability of direct threat occurrence for an agent i, when its security level is x_i ($\mathbf{pr}_i^{dir} = \pi_i(x_i)$). Let also $h_{i,j}$ be the probability of contagion of node i by a compromised node j. Thus, the probability for a node i to be compromised through contagion only (indirectly) is: $\mathbf{pr}_i^{cont} =$

$1 - \prod_{j \neq i}(1 - h_{i,j} \times \pi(x_j))$. To find the overall probability of accident for an agent i we should consider both events [148, 106]:

$$\mathbf{pr}_i = 1 - (1 - \mathbf{pr}_i^{dir})(1 - \mathbf{pr}_i^{cont}) = 1 - (1 - \pi_i(x_i)) \times \prod_{j \neq i}(1 - h_{i,j}\pi_i(x_j)) \quad (8)$$

The network is modelled with a topology model, which defines how nodes are connected. Mathematically, the topology affects the probability of contagion. If a connection between two nodes does not exist this probability is zero. The following topologies are usually considered in the literature:

- *independent nodes* [106, 79, 109, 110]. In this case no connections exist between nodes $\forall i, j \ h_{i,j} = 0$ and they can be considered separately.

$$\mathbf{pr}_i = \pi_i(x_i) \quad (9)$$

- *complete graph* [106, 29]. In this graph every node is connected to any other node, e.g., $\forall i, j \ h_{i,j} \geq 0$. There are two particular cases of this topology. The first one is when the probability of contagion is equal for each pair of nodes: $\forall i, j \ h_{i,j} = q$. In this case the overall probability is [106]:

$$\mathbf{pr}_i = 1 - (1 - \pi_i(x_i)) \times \prod_{j \neq i}(1 - q\pi_i(x_j)). \quad (10)$$

  Another case is a graph containing only two nodes [106, 30, 29]. Then, the overall probability is:

$$\mathbf{pr}_i = 1 - (1 - \pi_i(x_i)) \times (1 - q\pi_i(x_j)). \quad (11)$$

- *random graph (Erdös-Rényi graph)* [148, 84, 30]. Random graph is a graph with a specified amount of nodes where existence of an edge between two nodes is determined probabilistically (e.g., with a specified probability).

- *other models* [84, 29, 27]. Several other models are also could be of potential interest, although are not frequently considered by authors: tree-shaped topology [84], star-shaped topology [29], structured clusters [27].

4.3 Insurability analysis of cyber risks

Several studies [47, 39, 24] analysed cyber risks according to the criteria of insurability given in Section 2.3.1. They have found that although cyber risk has some problems with satisfying several criteria, in general, cyber risk can be insured, although more work is to be done to make cyber insurance market more mature.

We have collected the results of the studies in Table 2. We color the criteria found to be non-problematic in white, moderately problematic - in light grey

Sub-phase	Steps	Criteria of [20, 39, 24]	Criteria of [91, 47]	Open issues
Risk Identification	Asset Identification			evolution of systems lack if experience and standards
	Threat identification			evolution of systems lack if experience and standards
	Security/ Vulnerability identification			evolution of systems lack if experience and standards
Risk Analysis	Likelihood determination	Loss Exposure	Large number of similar exposure units	Evolution of attacks
		Randomness of loss occurrences	Accidental loss	Interdependence of security
		Information Asymmetry		Information Asymmetry
			Calculable loss	Hard to specify rate of occurrences Lack if statistical data
	Impact Determination	Average loss per accident	Large loss	Hard to estimate damage
			Calculable loss	Hard to estimate damage
			Definite loss	Hard to estimate damage
		Maximum possible loss	Limited risk of catastrophically large accidents	Hard to estimate damage
	Risk Estimation			Hard to verify
Establish Contract	Coverage Specification	Coverage Limits		Unclear coverage Exclusions and limited coverage Low indemnity limits
	Premium Estimation	Insurance premium	Affordable premium	correlated risks
	Write & Sign Contract	Public Policy Legal restrictions		language overlapping with existing insurance coverage liability

Table 2: Impact of problematic issues on insurability of cyber risks.

and problematic as dark grey. The table also shows which steps of the insurance process are affected by problems in satisfying the criteria, and how these criteria relate to the issues identified in our paper.

Table 2 indicates, that the most threatening issues are randomness of loss occurrences, information asymmetry, and coverage limits. We see, that the coverage limits issue coincides with the actual complains of the insureds (see Section 3). Also the importance of the information asymmetry issue can be seen in many scientific papers on the matter (see Section 5). As for randomness of loss occurrences, then here the conclusions of the informal analysis of ENISA [47] and C. Biener et. al. [39, 24] do not coincide well. ENISA is more optimistic on the matter, but agrees that interdependence of security and correlation of risks have a big impact on the cyber insurance market.

5 Analysis of the Literature

In this section we summarise the main articles relevant for cyber insurance. We start with risk management methodologies to list the current practices and

proposed methods for risk assessment and treatment. Then we outline the main problems of cyber insurance targeted by the research community and aggregate the findings in a unified way.

5.1 Risk/Security level specification

Cyber risk management. Risk management guidelines [92, 41, 8, 140] contain generic methodologies for the process. They devote particular attention to organisational questions related to the process, like the description of the parties involved in the process, definitions of the main terms, the supporting documents, and high level description of the phases. Although, the guidelines often have the primary focus on the risk assessment and risk treatment phases, they also include other activities, like implementation of treatments [92, 8], communication of results [41], monitoring and assessment [8, 92, 140], maintenance and improvement [8]. In this respect, the overall cyber risk management process can be seen as a specific application of the widely-known Plan-Do-Check-Act (PDCA) cycle. Moreover, the famous ISO/IEC 27001 standard [73] can also be seen as a risk management guideline since it describes all steps for risk management, including risk assessment and risk treatment.

Some of the guidelines are generic and do not go deep into the risk assessment and risk treatment phases [140, 41], when others go even further and next to the specific guidelines describe possible techniques [8] and even provide tools for risk assessment [92].

Cyber risk assessment and treatment. There are a number of approaches [37, 8] which define and help to implement risk assessment and treatment phases of risk management. Although every approach defines the steps with a slightly different level of details and may use different names for them, the overall process flow is always the same and equal to the one defined in Section 2.3 for Phase 0. In contrast to specific techniques, discussed below, these approaches are complete, i.e., cover all steps of the phase in a unified method. Nevertheless, many guidelines also propose to use specific techniques to easy the fulfilment of specific steps.

The first revision of NIST SP 800-30 [104] made the methodology, previously devoted to the risk management process, more focused on risk assessment, although such topics as risk sharing and maintaining the risk assessment are also considered. The revision is not a comprehensive approach, but it provides a high level description of the risk assessment process and proposes catalogues of expert knowledge helpful for every step of the phase. The risk management guide by Microsoft [92] also contains mostly the high level descriptions of steps, but it is also supported by different tables and worksheets to fill in.

Hazard and operability study (HAZOP) [69] and Failure mode and effects analysis (FMEA) (and its extension Failure mode, effects and criticality analysis (FMECA) [32]) are table-based approaches for risk analysis widely known by reliability engineers. The general idea behind these approaches is to list the main concepts of risk assessment (e.g., causes/threats, consequences/impact, possible

safeguards etc.) in columns where a row will specify a concrete scenario. In contrast to HAZOP, FMEA/FMECA also takes into account the probability of the scenario and its severity.

Operational Critical Treat, Assets, and Vulnerability Evaluation, OCTAVE Allegro [37], is the latest version of a well-defined and widely-known risk approach for risk assessment. The approach employs workshop-based data collection using a set of pre-defined worksheets and is supported by questionnaires. OCTAVE Allegro is mainly a qualitative or semi-quantitative approach. Although the approach can define threat and impact levels quantitatively the aggregation of these values are dubious from the mathematical point of view. Similar to OCTAVE Allegro, MAGERIT methodology [8] also contains a risk assessment approach based on filling in predefined worksheets, mainly during the meetings and interviews with the stakeholders. The methodology also provides a catalogue for possible assets, threats, vulnerabilities and their assessment.

Mehari 2010 [42, 43, 44] is a checklist based approach with a knowledge base support to risk analysis. The approach provides a set of tables for steps of the analysis with the questions originated from the ISO 27002:2005 standard [72]. Thus, the approach provides the analysis without any protection and with protection. The Mehari knowledge base provides various support (e.g., propose threat scenarios, intrinsic likelihood, intrinsic impact, risk reduction values, etc.).

CORAS [86, 52, 139, 57, 33] is a framework for model-based security risk analysis. The framework consists of three parts: a language, a method, and a tool. The language is a graphical representation of the main concepts and relations between them. The method is an asset-driven defensive risk analysis which is supported by the tool implementing the language. The main concepts of risk assessment (such as threat agents, threats, vulnerabilities, impact, assets, etc.) are represented as nodes of specific types and are connected with relations between them. Quantitative or qualitative values may be assigned to the nodes and relations for risk evaluation.

S. Butler [35] proposed a cost benefit analysis method called Security Attribute Evaluation Method (SAEM). The method is based on the multi-attribute assessment, where analysis is performed using several criteria at the same time. For example, impact of different threats is considered using four criteria: loss of productivity, loss of revenue, regulatory penalties, and reputation. The overall impact for a threat is a weighted sum of these losses. A similar analysis is performed for selection of the most appropriate protection strategy. Countermeasures are selected depending on how well they mitigate risk, how costly they are, and how much maintenance they require.

Karabacak and Sogukpinar [78] introduced Information Security Risk Analysis method (ISRAM). ISRAM is a quantitative approach that uses questionnaire results to analyse security risks. The method proposes to weight the answers of the interviewed persons. Then the likelihood and impact are determined as average (with respect to the amount of interviewed people) of these values.

Another approach based on a security risk questionnaire is proposed by Bennett and Kailay [19]. The authors proposed a questionnaire, that should

provide the main data for risk assessment. A similar approach for processing the results of a checklist analysis was proposed by F. Farahmand et. al [50].

Risk analysis techniques. Analysis of *business documentation* [8, 104] is a way to determine the most important assets. Various documents and models may be taken into account, e.g., data flow charts, process charts, enterprise architecture, inventory lists, etc.

Meetings, interviews. The most obvious way of getting the required information for every step of the risk assessment is to ask the stakeholders. This can be done in a form of *meetings* and *interviews* [37, 8, 86]. *Questionnaires* [78], *checklists* [42, 43, 44, 50] and *worksheets* [37] can be the instruments to structure the knowledge received during such meetings, as well as filled in by the stakeholders themselves. *Delphi method* [66] can be helpful to increase the credibility in the results of the interview. The method allows stakeholders to reconsider their evaluation after reviewing the results of others.

A *knowledge base* [42, 43, 44, 104, 37, 8] is a technique to identify assets, threats and vulnerabilities, assess the impact and the probability, define threat scenarios and propose possible safeguards. The knowledge base is created by experts in the field an provide the common practice knowledge to be re-used in concrete cases.

Threat trees [115, 37], *fault trees* [70, 86, 104], and *attack trees* [127, 89, 8, 86, 104] are the know techniques to specify threats relevant for an agent. All these trees have the general threat as a root and then step by step make it more and more specific. Attack trees are the fault trees applied in the area of cyber security. The difference between attack trees and threat trees is negligible (if exists at all). A threat tree has similar ways to decompose the threats per a tile (e.g., by actors, motive, outcomes), when an attack tree is more flexible and allows any kind of decomposition. *Defense trees* [25] is the extension of attack trees, when possible countermeasures are attached to the leaves of the attack tree.

History/log analysis [104, 92] is the best way to determine the likelihood of an accident, assuming that the likelihood will not change in the future and the statistics is significant for the analysis.

Standards and *certifications.* Having cyber security certifications is also a way to demonstrate that certain requirements and controls have been implemented according to appropriate standards. In particular, management standard ISO/IEC 27001:2013 [73] is the most well-known security standard. The standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of organization. Other cyber security standards which can be of interest are: ISO/IEC 13335-1 [146], ISO/IEC 21827:2008 Systems Security Engineering - Capability Maturity Model (SSE-CMM), COBIT framework (Control Objectives for Information and related Technology) [141], IASME [67], etc. Moreover, standards for specific domain which contain security requirements also can be reused, e.g. ISO/TS 16949:2009 [74] for automotive industry, the

North American Electric Reliability Corporation (NERC) Reliability Standards for Bulk Electric System (BES)[103], standard NEN 7510:2011 [102] and HIPAA for healthcare, ISO/IEC 27018:2014 [71] for cloud. Some insurance companies have reached agreements with certification bodies and are more willing to reduce premiums if their products are certified. For example, AIG has launched a cyber product for SMEs in conjunction with broker Sutcliffe & Co and IASME Consortium to support the governments Cyber Essentials Scheme [95].

Event tree analysis (ETA) [68] and *attack graphs* [107, 135, 105, 117, 82, 18]. ETA represents consequence of events as a tree, where every tile in the tree is a specific event which can be successful or not. This technique is useful to analyse possible outcomes of an accident and compute its probability. Attack graphs are the graphs formed by existing vulnerabilities/exploits connected according to their pre-conditions and effects. The set of vulnerabilities to be used in attack graphs can be found with vulnerability *scanning tools* (e.g., [137]).

Annualised Loss Expected (ALE) [55, 92] analysis and *risk tables* [104, 86]. A common way to compute risk quantitatively is to use the ALE analysis. This analysis is base on Equation 1, and uses Annualised Rate of Occurrences (ARO) (an average amount of accidents in a year) and Single Loss Expectancy (the average loss per accident):

$$ALE = ARO \times SLE \tag{12}$$

For estimation of risks with qualitative parameters *risk matrix* [140, 86, 104] are used, which map a likelihood level and impact levels to a pre-defined (by experts or stakeholders) risk level.

Cost benefit analysis [55, 140] and *Return on Security Investments* [48]. The cost benefit analysis shows the benefits in saved expenditure because of installation of a security control. Let ALE_b be the ALE value before installation of the control, when ALE_a - after the installation and $cost_c$ be the cost of the control. Then,:

$$CBA = ALE_b - ALE_a - cost_c \tag{13}$$

ROSI shows the expenditure effectiveness of the control:

$$ROSI = CBA/cost_c \tag{14}$$

Coverage analysis [35, 36]. S. Butler proposed a *coverage analysis*, which is based on the ideas of defence-in-depth and defence-in-breadth. The need of a countermeasure is determined on the basis of having at least some protection against all most dangerous risks and heaving protection mechanisms on different levels: protect, detect, recover.

Table 3 shows the techniques which could be found helpful for performing specific steps of the risk assessment and treatment process. The techniques for risk assessment are the same for Phases 0 and 1, although, as it has already been pointed out, often much less real data are available for the analysis at Phase 1 than at Phase 0. On the other hand, an insurer, which has a wider knowledge

about claims per similar insureds, may have much more reliable knowledge databases and more experience in conducting the analysis, in general.

5.2 Contract Specification and Contract Establishment

An insurer and an insured should agree on the terms and conditions in order to specify a contract. In particular, from the point of view of the mathematical model of cyber insurance, it is important to specify the threats covered by insurance (*coverage*) and the *indemnity* to be repaid in case of a covered accident. Then, the contract is estimated and the premium is computed.

In most cases these steps are performed with a simple action of an agent by selecting one of the insurance policies pre-defined by the insurer (e.g., [4, 143, 65, 121] On the other hand, for special customers insurers may apply individual approaches and define a custom policy by meeting with the client and discussing coverage and indemnity in details. Although, these approaches are significantly different from a practical point of view (e.g., in terms of resources required for contract specification), there is not much difference from the perspective of the mathematical model. Mathematically, both partners should consider the deal from a game theory point of view and come to a conclusion that signing the contract is profitable for both parties. The insured should select the amount of indemnity to maximize its utility. The insurer should either behave in accordance to its regulatory function (e.g., when it is a zero-profit organisation) or to maximize its benefits (or utility). Naturally, in reality, this rigorous mathematical analysis is hidden behind the pre-defined contracts and price limits set up for negotiators by their back offices.

Table 4 contains the steps for Contract Specification sup-phase of Phase 1. In this table we do not repeat the assessment part, since it is the same as for Phase 0 (`Self-Assessment and Treatment by an Agent`).

5.3 Contract Specification with Independent Security

From the high level point of view, specification of cyber risk insurance policy does not differ much from other types of risk defined in Section 2. Next to the simplistic application of insurance to cyber risks [96, 97, 125] several interesting problems were considered.

Secondary losses and information asymmetry. Bandyopadhyay et al. [16, 15] analysed the proposed model under different scenarios (information symmetry and asymmetry) of the cyber insurance market. A particular attention of the study was devoted to secondary losses associated with a cyber accident. The results of the study shows how the secondary loss exposure affect insured companies, generate information asymmetry between the insurer and the insured companies, and impede the development of cyber insurance.

Cyber insurance and social welfare. Kesan et al., [79] provided an experimental method to prove that cyber insurance improves security and social

Sub-phase	Steps	Technique
Risk Identification	Asset Identification	business documentation meetings/interviews questionnaires/checklists/worksheets knowledge base
	Threat identification	business documentation meetings/interviews questionnaires/checklists/worksheets knowledge base Threat trees/FTA/Attack trees
	Security/Vulnerability identification	ETA Attack graphs vulnerability scanning penetration testing meetings/interviews questionnaires/checklists/worksheets knowledge base Delphi method
Risk Analysis	Likelihood determination	History/log analysis meetings/interviews questionnaires/checklists/worksheets knowledge base Delphi method
	Impact Determination	meetings/interviews questionnaires/checklists/worksheets knowledge base Delphi method
	Risk Estimation	Risk table ALE
Risk Treatment	Risk prioritization	Criteria analysis
	Identification of treatment	meetings/interviews questionnaires/checklists/worksheets knowledge base Delphi method Defense Trees
	Prioritisation of Treatment	meetings/interviews questionnaires/checklists/worksheets knowledge base Delphi method Cost-benefit analysis/ROSI Coverage analysis
	Implementation of Treatments	

Table 3: Techniques for Phase 0 (Self-Assessment and Treatment by an Agent).

Sub-phase	Steps	Technique
Contract Specification	Coverage Specification	selection by agent meetings Game theory
	Premium Estimation	Game theory
	Write & Sign Policy	paper work signature

Table 4: Techniques for the Contract Specification and Establish Contract sub-phases of Phase 1.

welfare, if security of agents is not interdependent. R. Pal and L. Golubchik [109] analysed the problem from the perspective of an insurer: they have found that a selfish monopolistic insurer charges higher premiums to the users and gets more profit with respect to the welfare-maximizing insurer.

Security and non-security risks. R. Pal et al., [110] proposed Aegis, a cyber insurance model, for the cases when an agent is not able to distinguish security (insurable) and non-security (non-insurable) losses. The authors have shown that if insurance is mandatory for agents, then the agents are going to choose the Aegis contract in the specified settings.

5.3.1 Interdependent Security

Our unified approach to analysis of the literature. We organise diverse studies on the effect of interdependence of security on cyber insurance in a form of a table to analyse the papers in a unique fashion. The table has three main parts: *pre-conditions*, the applied *mathematical method*, and *results*. *Pre-conditions* define the concrete settings for the considered case study and, thus, the case study itself. Since, many papers apply their analysis to different situations, we split the corresponding column in the corresponding amount of parts.

The preconditions have been formally defined in Section 2.2 and here we simply define the symbols used in the table.

Market type - Three types are considered: monopolistic (M), competitive (C), and immature market (C^*);

Coverage - The insurance coverage can be *full*, *part*ial or both types (*ind*) of insurance coverage. By (*ind*)ifferent coverage we also mean the situations, when agents are allows to select the portion of the insurance to buy;

Mandatory - Insurance can be either mandatory (✓) or volatile (X);

Correlated risk and interdependent security - Although, the goal of our study is to consider the case of interdependent security we also left some independent cases for comparison.

Profit of insurer - An insurer may have *non-zero* profit (NZ), (*max*)imised profit or does not have profit at all (*ZP*);

Information asymmetry - We mark the type of information asymmetry considered by authors (moral hazard (*MH*), adverse selection (*AS*), or both *MH+AS*) and put *X* otherwise;

Topology - The following network topologies were found in the literature: *total*, 2 nodes, Erdös-Rényi graph (*ERG*), t-copula for global and Bernoulli Binomial for intra-firm dependency (t-copula/BB)[4]. If the authors use the general model for topology we write *ind*.

Homogenity - When agents are homogeneous we mark it with (✓) and put (*X*) when agents are heterogeneous.

Corrective treatment - For the cases when some regulatory action is applied, we indicate this in one of the following ways: Fines and Rebates (*F*/*R*), additional *tax* for low self-protection, liability for contagion (*L*), Risk Pooling Arrangements *RPA*, mandatory investment level *MIL*.

The applied *mathematical method* defines the concrete mathematical treatment which was used for the analysis. In most cases the authors stated only that Nash equilibrium (*NE*) had to be found. Also Monte-Carlo method *MC*, Bayesian Network Game (*BNG*), Walrasian Equilibrium *WE* were applied.

Although, the authors considered different case studies, i.e., situations with difference pre-conditions, we can single out main results targeted in most of the papers.

existence of equilibrium - This simple problem considers whether it is possible to come up with a set of variables which do not allow any of the participant to deviate from the specified behaviour and get more profit than in the case of equilibrium.

existence of market - This problem specifies whether the market defined by pre-conditions may exist. In particular, here we focus on the case where some agents prefer the insurance case to non-insurance. In short, if $E[U^I]$ is the average utility of some agent with insurance and $E[U^N]$ - without it, then $E[U^I] \geq E[U^N]$. Naturally, in case of mandatory insurance such analysis is meaningless.

Incentive for self-protection - This problem checks whether the cyber insurance is an incentive for increasing investments in self-protection. In

[4]In fact, the model of R. Böhme and G. Kataria [27] is more complex and also takes into account the time of accidents.

short, if the security level of a potential insured with insurance is x^I and it is x^N without it, then $x^I \geq x^N$. We say that cyber insurance is an incentive if all insurance buyer increase their self-protection, and partial if only some of them do.

Reaching social welfare - This problem focuses on the society as a whole, comparing the level of security investments (security levels) in case of maximisation of individual utility and utility of the society. Let security level in the former case be x^* and in the later one x^+, then we would like to have $x^* = x^+$. Note, that the case $x^* > x^+$ is as well undesirable as $x^* < x^+$, because the former case means over-investing in security [150].

Incentive for social welfare - This problem studies the difference between the social optimum levels of the situations when cyber insurance is provided ($x^{+,I}$) and when no cyber insurance is available ($x^{+,N}$). Naturally, it is desirable to have $x^{+,I} > x^{+,N}$.

In our analysis, we mark it as (✓) if a specific result was achieved and (X) if it was not. The problems not considered by the authors are marked with "-".

For the convenience of representation we broke our analysis in three parts. First, we analyse the competitive market. Then, we show our results for non-competitive and monopolistic markets. Finally, we study all types of markets with applied corrective treatment.

Competitive market In a perfectly competitive market there exists a large number of sellers (insurers) and no new seller is able to provide a contract more attractive for buyers that the ones already existed [113].

Table 5 summarizes some cases described by different authors who analyzed cyber insurance under competitive insurance market.

We start with an analysis of the literature with a naive model of competitive market (Table 5). Table 5 shows that the optimum security level maximizing individual utility can reach the optimum security level maximizing social welfare only when a complete symmetry exits between agents [130]. On the other hand, H. Ogut et al., [106] with similar pre-conditions came to opposite conclusions. One possibility for this contradiction could be a slightly different model of large-scale networks used by G. Schwartz and S. Sastry, but a more thorough investigation is required.

Another finding that follows from Table 5 is that cyber insurance is not an incentive for cyber security investments. Thus, with cyber insurance available, agents prefer buying insurance rather than investing in self-defence. Consequently, the social optimal levels of investments with insurance are also below the levels without it.

There is only one exception from this generic rule: with no information asymmetry Yang et al., [148] show both formally and empirically that security could be an incentive for security investments if specified conditions are satisfied. In contrast, Ogut et al., [106] came to a conclusion that under the same conditions

Table 5: Summary of approaches with competitive market model.

	Topic	Papers										
		[150]	[106]		[148]			[85]	[134]/[133]	[130]	[128]/[129]	[113]
Pre-conditions	Market type	C	C	C	C	C	C	C	C	C	C	C
	Coverage full	full	ind	ind	ind	full	part	ind	ind	ind	ind	full
	Correlated risk/ Int. security	✓	X	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Profit of insurer	zp	zp	zp	zp	zp	zp	zp	zp	zp	zp	zp
	Information asymmetry	X	X	X	X	MH	MH	MH	MH	MH	AS	MH+AS
	Topology	ind	-	Total	ERG	ERG	ERG	ERG	Total	Total	Total	Total
	Homogeneity of agents	✓	✓	✓	✓	✓	✓	X	✓	✓	X	X
	Mandatory insurance	X	X	X	X	X	X	X	X	X	X	X
	Corrective treatment	X	X	X	X	X	X	X	X	X	X	X
	Math. method	NE	NE	NE	BNG	BNG	BNG	NE	NE	NE	NE	WE
Results	Existence of equilibrium	✓	✓	✓	✓	X	✓	X	✓	✓	✓	✓
	Efficiency of market	-	✓	✓	✓	X	✓	-	✓	✓	✓	✓
	Incentive for self-protection	-	-	X	part	X	X	X	X	X	X	X
	Reach social optimum	X	-	X	-	-	-	-	-	✓	-	X
	Incent. social optimum	-	-	-	-	-	-	-	X	X	-	-

there is no possibility for insurance to be positive incentive for self-protection investments. One possible explanation of this mismatch could be that Yang et al., [148] considered discrete model for security investments (i.e., an agent may either invest into security or not), while Ogut et al., [106] evaluated a model with continuous investments, which allows every agent to spend the optimum amount for self-protection. Another possibility could be the difference in models: random graphs result in different effects on interdependency for agents, while total model assumes equal impact.

Finally, Yang et al., [148] and M. Lelarge and J. Bolot [85] contradict to N. Shetty et al., [134, 133] in the possibility for the equilibrium to exist for similar cases. One possible explanation for the fact that N. Shetty et al., [134, 133] were able to find an equilibrium could be the fact that in their work the authors consider homogeneous agents with complete network connections (e.g., all parameters and effects of externalities are the same for all actors, which leads to the same decisions), while M. Lelarge and J. Bolot [85] consider heterogeneous agents (with different effects of investments on self-protection), when Yang et al., [148] use random graph as a model of the network topology, rather than symmetric total graph.

Non-Competitive market Competitive market is a convenient but a naive model. In reality, the market is not competitive. Insurance carriers are greedy as well as the insured agents, they need some safety capital in order to avoid bankruptcy because of a large number of simultaneous claim demands, cover administrative costs, etc. Thus, two other market models are also considered

in the literature: monopolistic insurer and immature market (as defined in Section 4.2). We summarized the main findings for the immature market in Table 6.

Table 6: Summary of approaches with non-competitive market model.

	Topic	Papers							
		[27]	[106]		[136]	[85]	[108]		[113]
Pre-conditions	Market type	C*	C*	C*	C*	M	M	M	M
	Coverage full	ind	ind	ind	ind	part	part	part	full
	Correlated risk/ Int. security	✓	X	✓	✓	✓	✓	✓	✓
	Profit of insurer	NZ	NZ	NZ	NZ	max	max	max	NZ
	Information asymmetry	X	X	X	X	MH	MH	AS	MH+AS
	Topology	t-copula/ BB	-	Total	Total	ERG	ind	ind	Total
	Homogeneity of agents	✓	✓	✓	✓	X	X	X	X
	Mandatory insurance	X	X	X	X	X	✓	✓	✓
	Corrective treatment	-	-	-	-	-	-	-	-
	Math. method	MC	NE	NE	NE	NE	BNG	BNG	NE
Results	Existence of equilibrium	✓	✓	✓	✓	✓	✓	✓	✓
	Efficiency of market	-	✓	✓	✓	✓	-	-	-
	Incentive for self-protection	-	✓	X	X	X	-	-	X
	Reach social optimum	-	-	X	-	-	-	-	X
	Incent. social optimum	-	-	-	-	-	-	-	

We see that these types of market have received less attention by the authors. A few studies suggest that the immature market is also not a good incentive for self-protection [85, 113] and that the optimal values do not maximize the social welfare [106, 113]. Even the mandatory insurance does not improve the situation [108, 113]. Probably, this inability to solve these problems forced authors to devote more attention to application of different corrective treatments in context of these markets. Nevertheless, here we can underline that the available studies show that the insurer is able to make positive profit even in presence of information asymmetry and be attractive for the agents [106, 85, 108, 113].

It is important to note, that although the pre-conditions in Table 6 for H. Ogut et. al [106] and W. Shim [136] are similar, the later paper also provides a model for negative externalities. This is the only example of the model for negative externalities we were able to find (apart of a generic study by X. Zhao et. al, [150]). W. Shim [136] has shown that the negative externalities are more relevant for targeted attacks, when the possibility of untargeted attacks (e.g., virus) creates positive externalities. Nevertheless, the results of the analysis show that even in this situation insurance is not a good incentive for self-protection.

Corrective Treatments We saw that for all types of market, in contrast to opinions of security researchers [142, 100, 88, 126, 11], cyber insurance is neither a good incentive for self-investment nor is a mechanism to reach social

welfare. Therefore, researchers studied whether some regulatory treatments of the market can improve the situation. The results are summarized in Table 7.

Table 7: Summary of approaches with corrective treatment

	Topic	Papers												
		[98]		[85]					[30, 29, 31]	[106]	[113]	[150]	[134, 133]	[128, 129]
Pre-conditions	Market type	M	M	M	M	M	C	C*	M	C*	M	C	C	C
	Coverage full	ind	ind	full	full	full	full	full	full	part	full	part	full	ind
	Correlated risk/ Int. security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Profit of insurer	ZP	ZP	MAX	NZ	ZP	ZP	NZ	NZ	NZ	NZ	ZP	ZP	ZP
	Information asymmetry	X	X	X	X	X	X	X	X	X	MH+AS	MH	MH	AS
	Topology	ind	ind	ERG	ERG	ERG	ERG	ERG	Total	2 nodes	Total	ind	Total	Total
	Homogeneity of agents	X	X	X	X	X	X	X	X	✓	X	✓	✓	✓
	Mandatory insurance	✓	X	X	X	X	X	X	X	X	✓	X	X	X
	Corrective treatment	F/B	F/B	F/R	F/R	F/R	F/R	F/R+ tax	F/B	L	F/B	RPA	MIL	MIL
	Math. method	NE	NE	NE	NE	NE	NE	NE	NE	NE	NE	NE	NE	NE
Results	Existence of equilibrium	✓	✓	✓	✓	✓	X	✓	✓	✓	✓	✓	✓	X
	Efficiency of market	-	X	✓	✓	✓	-	✓	✓	✓	-	✓	✓	-
	Incentive for self-protection	✓	X	X	✓	✓	X	✓	✓	-	✓	X	X	-
	Reach social optimum	✓	X	-	-	-	-	-	-	X	✓	-	X	-
	Incent. social optimum	-	-	-	-	-	-	-	-	-	-	-	-	-

First of all we see that using fines and rebates (F/B) for agents with low/high probability of losses is the most successful treatment in case of the non-competitive market. On the other hand, this treatment can be applied only when no information asymmetry is in place, since the insurer has to be able to observe the security protection of agents (at least a posteriori). Furthermore, the results show that insurer should not maximize its profit [85] (although non-zero profit is possible [85, 30, 29, 31]). Moreover, although the insurer can have positive profit and provide a contract which is an incentive for self-protection, the most profitable effect for the society is reached when the insurer has zero profit[85]. In the last case, the insurer only re-distributes the money from low security agents to the agents with higher security [98, 85, 113]. H. Ogut et al.,[106] also showed that if an agent caused contagion is made liable (L) for the consequences (i.e., has to repay losses to other) then the amount of investments in self-protection significantly raise and becomes higher than the optimal level for social welfare maximization problem (without liability). We see that it is not clear from the available studies whether mandatory insurance is required for operation of this mechanism [98, 113, 112, 111] or it is not [85, 30, 29, 31].

We also may see that the requirement for minimal investments does not help to make cyber insurance an incentive for self-protection in case of moral hazard or adverse selection problem in place [134, 133, 128, 129]. Similarly, risk pooling arrangements (RPA) cannot help to solve this problem either, although they may help to reduce over-investments if negative externalities have place [150].

Summary of main findings In short, we may summarize the main findings of the literature as follows:

- **Positive externalities caused by interdependence of security reduce the incentive for the insured to invest in self-protection if insurance option is available.**
- **Insureds would prefer to invest in self-protection only if the "fines and rebates" regulatory mechanism is applied and no information asymmetry exits. Moreover, in this case the insurer cannot not maximizes its profit.**
- **It is unclear where insurance can be served as a tool for approaching optimal level of investments. Many studies contradict on this point.**
- **Effect of heterogenity of nodes needs a more focused study.**

5.3.2 Other studies on cyber insurance

Here we summarise some interesting findings of the researchers which were not included in our overall analysis.

Reducing Monoculture effect. Bohme [26] proposed an idea to use cyber insurance for diversification of systems. Since monoculture may lead to interdependent risks, diversification will help to fight this drawback. Naturally, since the risk for non-dominating platform (e.g., Unix-based) is lower, then cyber insurers may assign lower premiums to such platforms. This could be another incentive for organisations to switch to an alternative platform. Also Pal and Hui [114] investigated a similar problems. Unsurprisingly, they came to a conclusion, that cyber insurers prefer to operate in a slowly changing environment.

Security provider as an insurer. S. Radosavac et al., [123] considered a model where a security provider is also a cyber-insurer and users are able to buy a portion of self-defence together with insurance. They came to a conclusion that there is no a definitive answer whether in case of interdependency of threats competitive market may exist. R. Pal et al., [112, 111] considered a similar model, but with the conditions of monopolistic insurer and enforced mandatory insurance. With a use of a specific utility function and Bonacich centrality measure the authors have shown that it is possible to define the pricing strategy maximizing the profit of the provider/insurer and convince the customers to buy some units of the self-defence product. X. Zhao et al., [150] investigated whether managed security service providers (MSSP) can also behave in a sort of insurer. They have shown that when all agents outsource their security management to one such provider then security investment become socially optimal.

Study the effect of externalities. H. Ogut et al., [106] investigated the effect of interdependency of threats and immaturity of the market on security investments with cyber insurance available. They have come to a conclusion that security investments fall with increase of the interdependency. A similar conclusions were also supported by other researchers [150, 136]. Furthermore, the incentive to self-protection rises with increase of immaturity of the market in some cases. This finding can be one more explanation why competitive cyber insurance market fails to improve the security levels of agents.

6 Research Gaps to Achieve

In this section we summarise the areas related to cyber insurance which need more attention of scientific community and practitioners. We structure our proposals according to the problematic issues of cyber insurance defined in Section 4.1 skipping those which mostly caused by lack of experience (since these problems will be automatically solved with the maturation of the market).

Evolution of systems. Dynamic cyber-insurance. Many IT technologies (e.g., Cloud, Social Networks, Mobile, Internet of Things, etc.) assume that environment is dynamic; this is especially related to providers of different services. This dynamicity has effect on the computation of the probability of an accident and increases the difficulty of assessment and re-assessment of the system, as well as other steps of the insurance process. In order to adapt to this condition cyber-insurance should become fast and adaptive, i.e., dynamic. The insurance process itself may re-use the power of cyber technologies, which it has to assess in its turn, to become agile. One may think about cyber-insurance as a kind of a service, which can be bought on-line.

Naturally, dynamic insurance will require (semi-)automatic insurance processes, including security level specification (e.g., dynamic risk assessment) and, probably, automatic claim handling. An organisation, which would like to have a cyber coverage for a long period may simply get sequential insurances, issued one after another one, unless it does not want it any more.

Information Asymmetry. New solutions. The analysis of the literature in Section 5.2 shows that information asymmetry is not only an obstacle for insurance, but also for security improvement as well. On the other hand, here IT technology may be of help for insurance. New ideas on Digital Right Management, Trusted computing, usage control, automatic certification etc., may be re-used to establish higher trust in the information provided by an insured and decrease the information asymmetry. Furthermore, cyber insurers may cooperate with service providers. The former provide insurance, the later install monitoring software on their platform.

Hard to specify rate of occurrences. Define security level and effect of security controls. Currently, most of the approaches start with a defined

"security level" or a function returning the probability of an attack depending on the security level. In the security literature there are no widely acceptable methods to find these values, required for cyber-insurance. There is a need for a deeper investigation on how defined security metrics [75, 63] affect the rate of occurrences and can be used to specify security level [81, 83].

Lack of statistical data. Increase information sharing capabilities. Lack of statistical data is mostly explained by the sensitivity of the information to be shared. Organisations are afraid of releasing too much information about their internal systems to prevent decrease of reputation as well as prevent leakage of knowledge about weaknesses of the system. The schemas assuring participants in absence of these potential problem are required. Moreover, it is required to think about possible incentives for organisation to engage in information sharing, instead of being dragged in it by the forces of the law.

Hard to estimate damage. New systematic approaches. Specification of possible damage is a known problem which exists for years in security risk assessment, yet still no comprehensive and reliable approach exists. It is even a problem to specify all possible effects a breach may have on the organisation, not speaking about determination of their magnitude.

Hard to estimate damage. Cyber insurance of unique systems. Although it is difficult to collect data for IT systems in use for some time, it is even harder to predict the losses when the system is unique as a cyber-physical system or an industrial control systems. One approach could be to re-use the information available for re-usable parts of the complex system and then aggregate it to get the estimation for the system as a whole. Such a modular risk management approach could help in cases when a big part of a novel system is composed of known devices.

Interdependency of security. New theoretical approaches and practical studies. From the analysis of the literature in Section 5.2 we saw that interdependent security has a negative impact on the incentive of the insured to invest in self-protection. The proposed approaches to market regulation work mainly without information asymmetry. Novel approaches to regulation of insurance market are required in order to mitigate this effect of externalities. Moreover, although the analysis of externalities has got a lot of attention in the scientific community there is a need to evaluate the real impact of interdependent security for every domain of insurance application. The real survey data show that despite gloomy theoretical predictions, cyber insurance is the incentive for increasing quality of protection [120].

Correlated risks. Evaluation the real impact. There are many studies of interdependent security, but security accidents correlate not only because of contagion, but also because of the nature of IT risks in general as well. The

threat of a "cyber hurricane" is of important concern for cyber insurance. the study of St. Gallen has shown that only 17% of attacks are somehow correlated. More empirical studies are required in order to evaluate the impact of the correlated threats. Moreover, as study by W. Shim [136] shows, the approaches for different threats may be different. These studies are important for all domains. Probably, the uniqueness of the cyber-physical and industrial systems makes these domains less affected by cyber hurricane outbreaks, but this possibility should not be eliminated completely in this domain either.

Correlated risks. Diversification. Currently, only a few studies are devoted to diversification of systems and its effect on cyber-insurance. In fact, they mostly consider a reverse problem: how cyber-insurance may help to diversify systems. What is required for cyber-insurance, is a way to diversify its coverage, in order to avoid or at least, reduce effects of possible cyber hurricanes.

Liability. Liability for potentially malicious actions of others. Many providers (ISPs, Cloud, Social Network providers) may be liable for not providing enough control over its customers and bare some responsibility for their malicious actions. The current schemas for cyber-insurance consider only insurer and insured, but in the considered situation also the end users of insured should be taken into account. Furthermore, service providers are involved into the forensics process that require additional resources to be allocated. Insurance may cover these losses and make providers more willing to cooperate with law enforcement agencies in order to improve the societal welfare.

Liability. Simplify forensics burden. Many insurers require official forensics to be conducted before reimbursing the expenses. This is not always feasible for small accidents (like virus penetration) covered by insurance, but not of primary importance for the law enforcement agencies. This is especially important for individuals or users of a service who have very limited resources and relatively small impact. A simple and convenient method for dealing with cyber accident notification and clue collection is needed.

7 Summary

In this paper we provided the most up-to-date comprehensive survey of available literature on cyber insurance. We have found, that despite a slow start and many problematic issues, the cyber insurance market grows. This growth much depends on the regulatory initiatives applied more widely in the world (e.g., the California bill), but this is not the only cause for the market to flourish. Cyber insurance by itself provides a unique opportunity to cover residual risk, as well as to contribute to societal welfare.

In this work we aligned many scientific contributions with a unique systematising view. Although, the view in no way can be seen as the only possible, fully descriptive and one size fitting all, it allows fast and easy comparison of various

studies in the field. The results of the comparison show that theoretically, cyber insurance by itself is not a good incentive for investments in self-protection. The main causes for this are information asymmetry and interdependent security. On the other hand, in some situations regulatory mechanisms can be applied to achieve the desired effect.

Finally, we proposed a number of possible directions for solving the existing issues. Some of these directions are well-known in risk assessment area (e.g., more precise determination of possible damage). But many of them are specific for cyber insurance, e.g., become more dynamic and use available technology to reduce information asymmetry. In some cases we have identified points, where practice and theory are not in line (e.g., whether cyber insurance is an incentive for self-protection investments or it is not) and where more real impact of theoretical issues should be confirmed (e.g., correlated risks and interdependent security).

8 Acknowledgements

This work was partially supported by the Unipol Gruppo Finanziario S.p.A. and projects H2020-MSCA-ITN-2015-NeCS 675320, and FP7-Camino 607406.

References

[1] ACE. Privacy and network security, 2015. Available via `http://goo.gl/eq1Ll2` on 13/07/2015.

[2] Advisen. Cyber insurance underwriting: A high-tech, evolving discipline, November 2014. Available via `http://goo.gl/LxoQDq` on 13/7/2015.

[3] Advisen. Cyber liability insurance market trends survey. Advisen Ltd., October 2014. Available via `http://goo.gl/oxZrK8` on 13/07/2015.

[4] AIG. Cyberedge cyber liability insurance - policy wording. Technical report. Available via `http://goo.gl/XH4hiL` on 29/10/2015.

[5] C. J. Alberts and A. J. Dorofee. OCTAVE Criteria. Technical Report CMU/SEI-2001-TR-016, CERT, December 2001.

[6] Allianz. Allianz cyber protect. Available via `http://www.agcs.allianz.com/services/financial-lines/allianz-cyber-protect/` on 13/07/2015.

[7] American Insurance Association. Propertycasualty insurance basics. available via `goo.gl/M06lRg`.

[8] M. A. Amutio and J. Candau. *MAGERIT- Methodology for Information Systems Risk Analysis and Management. Book I - The Method.* Ministerio de HJacienda Y Administraciones Publicas, 3.0 edition, July 2014.

[9] Armic. Airmic review of recent developments in the cyber insurance market. Technical report, Airmic Technical, 2012. http://goo.gl/JHpOZq.

[10] Australian Law Reform Commission. Data breach notification. Available via `http://goo.gl/ZZzan0` on 13/07/2015.

[11] W. Baer. Rewarding it security in the marketplace. *Contemporary Security Policy*, 24(1):190–208, April 2003.

[12] W. S. Baer and A. Parkinson. Cyberinsurance in it security management. *IEEE Security and Privacy*, 5(3):50–56, May 2007.

[13] L. Bailey. Mitigating moral hazard in cyber-risk insurance. *JL & Cyber Warfare*, 3:1, 2014.

[14] T. Bandyopadhyay. Organizational adoption of cyber insurance instruments in it security risk management a modeling approach. In *SAIS 2012 Proceedings*, 2012.

[15] T. Bandyopadhyay, V. S. Mookerjee, and R. C. Rao. Why it managers don't go for cyber-insurance products. *Communications of ACM*, 52(11):68–73, November 2009.

[16] T. Bandyopadhyay, V. S. Mookerjee, and R. C. Rao. A model to analyze the unfulfilled promise of cyber insurance: The impact of secondary loss. *Working Paper*, 2010.

[17] T. Bandyopadhyay and S. Shidore. Towards a managerial decision framework for utilization of cyber insurance instruments in it security. In V. Sambamurthy and M. Tanniru, editors, *AMCIS*. Association for Information Systems, 2011.

[18] K. Beckers, L. Krautsevich, and A. Yautsiukhin. Analysis of social engineering threats with attack graphs. In *Proceedings of the 3rd International Workshop on Quantitative Aspects in Security Assurance. To appear.*, Lecture Notes in Computer Science. Springer-Verlag, 2014. SESAMO, SECURE!, PRIN.

[19] S. P. Bennett and M. P. Kailay. An application of qualitative risk analysis to computer security for the commercial sector. In *Proceedings of 8th Annual Computer Security Applications Conference*, pages 64 – 73. IEEE Computer Society Press, 1992.

[20] B. Berliner. Large risks and limits of insurability. *The Geneva Papers on Risk and Insurance*, 10(37):313–329, October 1985.

[21] R. S. Betterley. Understanding the cyber risk insurance and remediation services marketplace. available via `http://www.casact.org/community/affiliates/CANE/0412/Betterley2.pdf` on 20/02/2015, 2010.

[22] R. S. Betterley. Cyber/privacy insurance market survey - 2014. available via `http://betterley.com/samples/cpims14_nt.pdf` on 23/03/2015, June 2014.

[23] R. S. Betterley. Cyber/privacy insurance market syurvey - 2015. available via `http://betterley.com/samples/cpims15_nt.pdf`, June 2015.

[24] C. Biener, M. Eling, and J. Wirfs. Insurability of cyber risk: an empirical analysis. available via `http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf` on 15/12/2014, 2014.

[25] S. Bistarelli, M. Dall'Aglio, and P. Peretti. Strategic games on defense trees. In *Proceedings of 4th International Workshop on Formal Aspects in Security and Trust*, pages 1–15, 2007.

[26] R. Böhme. Cyber-insurance revisited. In *Proceedings of the 4-th workshop on the Economics of Information Security*, June 2005.

[27] R. Böhme and G. Kataria. Models and measures for correlation in cyber-insurance. In *Proceedings of the 5-th Workshop on Economics of Information Security*, 2006.

[28] R. Böhme and G. Schwartz. Modeling cyber-insurance: Towards a unifying framework. In *Proceedings of the 9th Workshop on the Economics in Information Security*, 2010.

[29] J. Bolot and M. Lelarge. A new perspective on internet security security using insurance. Technical Report RR-6329, INRIA, 2007.

[30] J. Bolot and M. Lelarge. A new perspective on internet security using insurance. In *Proceedings of the 27th IEEE International Conference on Computer Communications,*, pages 1948–1956, Phoenix, AZ, USA, April 2008.

[31] J. Bolot and M. Lelarge. *Managing Information Risk and the Economics of Security*, chapter Cyber Insurance as an Incentive for Internet Security, pages 269–290. Springer US, 2009.

[32] A. Bouti and D. A. Kadi. A state-of-the-art review of fmea/fmeca. *International Journal of Reliability Quality and Safety Engineering*, 1994.

[33] F. Braber, I. Hogganvik, M. S. Lund, K. Stolen, and F. Vraalsen. Model-based security analysis in seven steps – a guided tour to the coras method. *BT Technology Journal*, 25(1):101–117, 2007.

[34] J. Bradford. 2015 network security & cyber risk management: The fourth annual survey of enterprise-wide cyber risk management practices in europe. Advisen Ltd., February 2015.

[35] S. A. Butler. Security attribute evaluation method: a cost-benefit approach. In *Proceedings of the 24th International Conference on Software Engineering (ICSE'02)*, pages 232–240. ACM Press, 2002.

[36] S. A. Butler. Security attribute evaluation method. Technical Report CMU-CS-03-132, Carnegie Mellon University, May 2003.

[37] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson. Introducint octave allegro: Improving the information security risks assessment process. Technical Report CMU/SEI-2007-TR-012, Software Engineering Institute, May 2007.

[38] E. Chabrow. 10 concerns when buying cyber insurance. BankInfoSecurity, June 2012. Available via `http://goo.gl/TT3Dqf` on 13/07/2015.

[39] M. E. Christian Biener and J. H. Wirfs. Insurability of cyber risk. *Newsletter on Insurance and Finance*, (14), 2014.

[40] Chubb. Cybersecurity for health care organizations. Available via `http://goo.gl/OqshT5` on 29/10/2015.

[41] CLUSIF. *Risk Management - Concepts and Methods*. Club de la securite de l'infromation francias, 30, rue Pierre Semard, 75009, Paris, 2009.

[42] CLUSIF. *Mehari 2010. Overview*. Club De La Securite De L;Information Francias, 2010.

[43] CLUSIF. *Mehari 2010. Risk analysis and tratment guide*. Club De La Securite De L'Information Francias, August 2010.

[44] CLUSIF. *Mehari 2010. Processing guide for risk analysis and managment*. Club De La Securite De L'Information Francias, 2 edition, April 2011.

[45] M. Crane. International liability in cyberspace. *Duke Law & Technology Review*, 1(1):23, 2001.

[46] J. Crowther, D. Dabbs, S. Dakin, A. M. Freed, R. Herold, R. Kam, C. Kallenbach, C. Marciano, A. I. Messing, E. Michel-Kerjan, M. Negus, W. Oravecz, L. Ponemon, R. Santalesa, H. Schneider, B. Schneier, and J. Westby. Data privacy, information security and cyber insurance trend. available via `goo.gl/MnbIUt` on 02/12/2014, 2013.

[47] ENISA. Incentives and barriers of the cyber insurance market in Europe. available via `goo.gl/BtNyj4` on 12/12/2014, June 2012.

[48] ENISA. *Introduction to Return on Security Investment*, December 2012.

[49] EY. Global insurance outlook. available via `goo.gl/uyFzQ4` on 11/08/2915.

[50] F. Farahmand, S. B. Navathe, P. H. Enslow, and G. P. Sharp. Managing vulnerabilities of information systems to security incidents. In *ICEC '03: Proceedings of the 5th international conference on Electronic commerce*, pages 348–354, New York, NY, USA, 2003. ACM.

[51] W. E. Forum. Global risks 2014. ninth edition. available via on 11/08/2015, 2014.

[52] R. Fredriksen, M. Kristiansenand, B. A. G. K. Stølen, T. A. Opperud, and T. Dimitrakos. The CORAS framework for a model-based risk management process. In *Proceedings of the 21st International Conference on Computer Safety, Reliability and Security*, volume 2434 of *Lecture Notes in Computer Science*, pages 94–105, 2002.

[53] D. Geer. Risk management is still where the money is. *Computer*, 36(12):129–131, Dec. 2003.

[54] N. Gohring. Cyberinsurance may cover damage of computer woes. The Seattle Times, July 2002.

[55] L. A. Gordon and M. P. Loeb. *Managing Cybersecurity Resources: a Cost-Benefit Analysis*. McGraw Hill, 2006.

[56] L. A. Gordon, M. P. Loeb, and T. Sohail. A framework for using insurance for cyber-risk management. *Communication of the ACM*, 46(3):81–85, Mar. 2003.

[57] B. A. Gran, R. Fredriksen, and A. P.-J. Thunem. An approach for model-based risk assessment. In *SAFECOMP*, pages 311–324, 2004.

[58] M. Greisiger. Cyber liability & data breach insurance claims. available via `goo.gl/6Xpoji` on 24/02/2015, 2013.

[59] A. Harrison. Counterpane offers internet security insurance. COMPUTERWORLD, July 2000.

[60] A. Hedrick. Cyberinsurance: A risk management tool? In *Proceedings of the 4th Annual Conference on Information Security Curriculum Development*, InfoSecCD '07, pages 20:1–20:4, New York, NY, USA, 2007. ACM.

[61] C. Hemenway. Broker beat: Fierce competition for more cyber buyers. ADVISEN NEWS, March 2014. Available via `http://www.advisenltd.com/insurance-news/2014/03/21/broker-beat-fierce-competition-cyber-buyers/` on 13/07/2015.

[62] H. S. B. Herath and T. C. Herath. Cyber-insurance: Copula pricing framework and implication for risk management. In *WEIS*, 2007.

[63] D. S. Herrmann. *Complete Guide to Security and Privacy Metrics. Measuring Regulatory Compliance, Operational Resilience, and ROI.* Auerbach Publications, 2007.

[64] D. Heywood. Data breaches what can we expect from the EU?, January 2015. Available via `http://goo.gl/6Sa38Z` on 13/07/2015.

[65] Hiscox. E-risks insurance- summary of cover. Available via `https://www.hiscox.co.uk/shared-documents/E-risks-insurance-summary-of-cover.pdf` 29/10/2015.

[66] C.-C. Hsu and B. A. Sandford. The delphi technique: Making sense of consensus. *Practical Assessment Research & Evaluation*, 12(10), 2007.

[67] IASME Consortium. The IASME Standard. Available via `https://www.iasme.co.uk/index.php/about` on 13/07/2015.

[68] IEC. *IEC 60300-3-9 Dependability management- Part 3. Application guide - Section 9: Risk analysis of technological systems - Event Tree Analysis (ETA)*, 1995.

[69] IEC. *BS IEC 61882:2001. Hazard and operability studies (HAZOP studies) Application guide*, 2001.

[70] IEC. *IEC 61025:2006. Fault tree analysis (FTA)*, 2006.

[71] ISO/IEC. Iso/iec 27018:2014 - information technology – security techniques – code of practice for protection of personally identifiable information (pii) in public clouds acting as pii processors. Available via `http://goo.gl/GnPUFG` on 13/07/2015.

[72] ISO/IEC. *ISO/IEC 27002:2005 Information technology – Security techniques – Code of Practice for Information Security Management*, 2005.

[73] ISO/IEC. *ISO/IEC 27001:2013 Information technology Security techniques Information security management systems Requirements*, 2013.

[74] ISO/TS. ISO/TS 16949:2009 - Quality management systems – Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations. Available via `http://goo.gl/9s4uGU` on 13/07/2015.

[75] A. Jaquith. *Security metrics: replacing fear, uncertainty, and doubt.* Addison-Wesley, 2007.

[76] S. Jones. Lloyds CEO Sees Cyber Insurance to Surge After Attacks. Bloomberg Business, October 2014. Available via `http://goo.gl/kN58LV` on 13/07/2015.

[77] M. E. Kabay. ICSA White Paper Threats, Vulnerabilities and Real-World Responses: The Foundations of the TruSecure Process. ICSA, Inc, 1998.

[78] B. Karabacak and I. Sogukpinar. Isram: information security risk analysis method. *Computers & Security*, 24(2):147–159, 2005.

[79] J. P. Kesan, R. P. Majuca, and W. J. Yurcik. The economic case for cybersinsurance. Technical Report LE04-004, Illinois Law and Economics, 2004.

[80] L. Krautsevich, F. Martinelli, and A. Yautsiukhin. Formal approach to security metrics. what does "more secure" mean for you? In *Proceedings of the 1st International Workshop on Measurability of Security in Software Architectures*. ACM Press, 2010.

[81] L. Krautsevich, F. Martinelli, and A. Yautsiukhin. Formal analysis of security metrics and risk. In *Proceedings of the IFIP Workshop on Information Security Theory and Practice*, volume 6633 of *Lecture Notes in Computer Science*, pages 304–319. Springer-Verlag, 2011.

[82] L. Krautsevich, F. Martinelli, and A. Yautsiukhin. Towards modelling adaptive attacker's behaviour. In *In Proceedings of 5th International Symposium on Foundations & Practice of Security*, volume 7743 of *Lecture Notes on Computer Science*, pages 357–364. Springer-Verlag, 2012. NESSOS, SESAMO.

[83] A. Y. Leanid Krautsevich, Fabio Martinelli. Formal analysis of security metrics with defensive actions. In *The 10th IEEE International Conference on Autonomic and Trusted Computing*. IEEE, 2013.

[84] M. Lelarge and J. Bolot. Network externalities and the deployment of security features and protocols in the internet. *SIGMETRICS Perform. Eval. Rev.*, 36(1):37–48, June 2008.

[85] M. Lelarge and J. Bolot. Economic incentives to increase security in the internet: The case for insurance. In *Proceedings of the 28th IEEE International Conference on Computer Communications*, pages 1494–1502, Rio de Janeiro, Brazil, April 2009.

[86] M. S. Lund, B. Solhaug, and K. Stølen. *Model-Driven Risk Analysis*. Springer, 2011.

[87] P. Luzwick. If most of your revenue is from e-commerce, then cyberinsurance makes sense. *Computer Fraud & Security*, 3:16–17, MArch 2001.

[88] R. P. Majuca, W. Yurcik, and J. P. Kesan. The evolution of cyberinsurance. *The Computing Research Repository*, abs/cs/0601020, 2006.

[89] S. Mauw and M. Oostdijk. Foundations of attack trees. In *Proceedings of the 8th International Conference on Information Security and Cryptology*, Lecture Notes in Computer Science. Springer-Verlag, 2005.

[90] T. Maynard. An overview of the cyber insurance market. available via http://www.acegroup.com/benelux-en/assets/risk-forum-2013_trevor-maynard_cyber-risk-14-march_v2-0.pdf on 24/02/2015, March 2013.

[91] R. Mehr and E. Cammack. *Principles of insurance*. Richard D. Irwin, inc., third edition edition, 1961.

[92] Microsoft. The security risk management guide. available via http://www.microsoft.com/en-us/download/confirmation.aspx?id=6232 on 25/06/2015, 2006.

[93] T. Mikosch. *Non-life insurance Mathematics*. Springer, 2009.

[94] T. Moore. The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, 3(3–4):103 – 117, 2010.

[95] C. Morrison. AIG offers SME protection against "hacktivists" with new cyber product, September 2014. Available via goo.gl/82zlnc on 13/07/2015.

[96] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, and S. K. Sadhukhan. Cyber-risk decision models: To insure it or not? *Decision Support Systems*, 56:11–26, Dec. 2013.

[97] A. Mukhopadhyay, G. K. Shukla, P. Kirs, and K. K. Bagchi. Quntifying e-risk for cyber-insurance using logit anf probit models. In *Proceedings of the 8th Annual Symposium on Information Assurance*, 2013.

[98] P. Naghizadeh and M. Liu. Voluntary participation in cyber-insurance markets. In *Proceedings of the 2014 Annual Workshop on Economics in Information Security*, 2014.

[99] National Protection and Programs Directorate. Department of Homeland Security. Cybersecurity insurance workshop readout report. available via https://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf on 24/03/2015, November 2012.

[100] National Protection and Programs Directorate. Department of Homeland Security. Cyber insurance roundtable readout report. health care and cyber risk management. cost/benefit apapproach. available via http://www.dhs.gov/sites/default/files/publications/February%202014%20Cyber%20Insurance%20Health%20Care%20Use%20Case%20Roundtable.pdf on 02/12/2014, February 2014.

[101] National Protection and Programs Directorate. Department of Homeland Security. Insurance industry working session readout report. insurance for cyber-related critical inftastructre loss: Key issues. available via

http://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf on 23/03/2015, July 2014.

[102] NEN. Nen 7510:2011 nl - health informatics - information security management in healthcare. Available via https://goo.gl/5pk0oT on 13/07/2015.

[103] NERC. Cip-002-4 cyber security critical cyber asset identification. Available via http://goo.gl/5i6zxg on 13/07/2015.

[104] NIST. Guide for conducting risk assessment. Technical Report SP 800-30 Revision 1, National Institute of Standards and Technology, September 2012.

[105] S. Noel and S. Jajodia. Managing attack graph complexity through visual hierarchical aggregation. In *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, pages 109–118, New York, NY, USA, 2004. ACM Press.

[106] H. Ogut, N. Menon, and S. Raghunathan. Cyber insurance and it security investment: Impact of interdependent risk. In *Proceedings of the 4-th Workshop on the Economics of Information Security*, 2005.

[107] R. Ortalo, Y. Deswarte, and M. Kaaniche. Experimenting with quantitative evaluation tools for monitoring operational security. *IEEE Transactions on Software Engineering*, 25(5):633–650, 1999.

[108] R. Pal. Cyber-insurance for cyber-security: a solution to the information asymmetry problem. In *Proceedings of SIAM Annual Meeting*, 2012.

[109] R. Pal and L. Golubchik. On economics of information security: The problem of designing optimal cyber-insurance contracts. In *Proceedings of ACM SIGMETRICS Workshop*, 2010.

[110] R. Pal, L. Golubchik, and K. Psounis. Aegis a novel cyber-insurance model. In J. Baras, J. Katz, and E. Altman, editors, *Decision and Game Theory for Security*, volume 7037 of *Lecture Notes in Computer Science*, pages 131–150. Springer Berlin Heidelberg, 2011.

[111] R. Pal, L. Golubchik, K. Psounis, and P. Hui. On a way to improve cyber-insurer profits when a security vendor becomes the cyber-insurer. In *Proceedings of the 12th IFIP Networking Conference*, pages 1–9, Brooklyn, New York, USA, May 2013.

[112] R. Pal, L. Golubchik, K. Psounis, and P. Hui. Realizing efficient cyber-insurance markets via price discriminating security products. available via http://www-scf.usc.edu/~rpal/TDSCR.pdf, 2013.

[113] R. Pal, L. Golubchik, K. Psounis, and P. Hui. Will cyber-insurance improve network security? a market analysis. In *Proceedings of the 2014 INFOCOM*, pages 235–243. IEEE, 2014.

[114] R. Pal and P. Hui. The impact of secure oss on internet security: What cyber-insurers need to know. Technical Report arXiv:1202.0885, CoRR, 2012.

[115] J. H. Pardue and P. Patidar. Threats to healthcare data: a threat tree for risk assessment. *Issues in Information Systems*, XII(1):106–113, 2011.

[116] E. Parliament. European parliament legislative resolution of 12 march 2014 on general data protection regulation, October 2014.

[117] C. Phillips and L. P. Swiler. A graph-based system for network-vulnerability analysis. In *Proceedings of the 1998 Workshop on New security paradigms*, pages 71–79. ACM Press, 1998.

[118] T. Poletti. First-ever insurance against hackers, June 1998. Available `http://goo.gl/SSGArI` on 13/07/2015.

[119] Ponemon Institute LLC. Managing cyber security as a business risk: Cyber insurance in the digital age. available via `http://assets.fiercemarkets.com/public/newsletter/fiercehealthit/experian-ponemonreport.pdf` on 02/12/2014, August 2013.

[120] PwC. Managing cyber risks in an interconnected world. availavle via `http://www.pwc.com/gsiss2015` on 14/08/2015, September 2014.

[121] QBE. Cyber and data security - proposal form. Available via `http://goo.gl/sEDlxc` 29/10/2015.

[122] QBE European Operations. QBE Cyber and Data Security. Available via `http://goo.gl/zaZf9E` 13/07/2015.

[123] S. Radosavac, J. Kempf, and U. C. Kozat. Using insurance to increase internet security. In J. Feigenbaum and Y. R. Yang, editors, *NetEcon*, pages 43–48. ACM, 2008.

[124] P. K. Rosen, B. Steinberg, M. K. Kearney, M. L. O'Connor, and N. A. Rubin. Cyber insurance: A last line of defence when technology fails. avilavle via `goo.gl/0NwDhO` on 19/10/2015, April 2014.

[125] D. K. Saini, I. Azad, N. B. Raut, and L. A. Hadimani. Utility implementation for cyber risk insurance modeling. *Proceedings of the World Congress on Engineering*, 1, 2011.

[126] F. B. Schneider. Enforceable security policies. *ACM Transactions on Information and System Security*, 3(1):30–50, 2000.

[127] B. Schneier. Attack trees: Modelling security threats. *Dr. Dobb's journal*, December 1999.

[128] G. Schwartz, N. Shetty, and J. Walrand. Cyber-insurance: Missing market driven by user heterogeneity. In *WEIS*, 2010.

[129] G. Schwartz, N. Shetty, and J. C. Walrand. Why cyber-insurance contracts fail to reflect cyber-risks. In *Proceeding sof the 51st annual Allerton Conference*, pages 781–787, 2013.

[130] G. A. Schwartz and S. S. Sastry. Cyber-insurance framework for large scale interdependent networks. In *Proceedings of the 3rd International Conference on High Confidence Networked Systems*, HiCoNS '14, pages 145–154, New York, NY, USA, 2014. ACM.

[131] S. J. Shackelford. Should your firm invest in cyber risk insurance? *Business Horizons*, 55(4):349 – 356, 2012.

[132] S. Shavell. *Foundations of Insurance Economics. Readings in Economics and Finance*, chapter On Moral Hazard and Insurance, pages 280–302. Springer.

[133] N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand. *Economics of Information Security and Privacy*, chapter Competitive Cyber-Insurance and Internet Security, pages 229–247. Springer US, 2010.

[134] N. Shetty, G. Schwartz, and J. Walrand. Can competitive insurers improve network security? In A. Acquisti, S. Smith, and A.-R. Sadeghi, editors, *Proceedings of the 3rd International Conference on Trust and Trustworthy Computing*, volume 6101 of *Lecture Notes in Computer Science*, pages 308–322. Springer Berlin Heidelberg, 2010.

[135] O. Sheyner and J. Wing. Tools for generating and analysing attack graphs. In *Proceedings of Formal Methods for Components and Objects*, Lecture Notes in Computer Science. Springer-Verlag, 2005.

[136] W. Shim. An analysis of information security management strategies in the presence of interdependent security risk. *Asia Pacific Journal of Information Systems*, 22(1), March 2012.

[137] Snort. Snort. `https://www.snort.org/`.

[138] C. State. Senate bill no. 1386 chapter 915. Available `http://goo.gl/W8qhb8` on 13/07/2015.

[139] K. Stolen, F. D. Braber, T. Dimitrakos, R. Fredriksen, B. A. Gran, S.-H. Houmb, S. Lund, Y. C. Stamatiou, and J. O. Aagedal. Model-based risk assessment the coras approach,. Proceedings of the 1st iTrust Workshop, 2002.

[140] G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems. Technical Report 800-30, National Institute of Standards and Technology, 2001. available via http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf on 13/05/2009.

[141] The IT Governance Institute. Cobit 4.1. Avalaible via http://goo.gl/OaxzmY on 13/07/2015.

[142] C. Toregas and N. Zahn. Insurance for cyber attacks: The issue of setting premiums in context. Technical Report GW-CSPRI-2014-1, The George Washington University, January 2014. available via http://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/53c3daa5e4b056f825681c72/1405344421345/cyberinsurance_paper_pdf.pdf.

[143] Travelers. Lawyers professional liability coverage declarations. Available via goo.gl/r2CXtB 29/10/2015.

[144] E. J. Vaughan and T. M. Vaughan. *Fundamentals of Risk and Insurance*. Wiley, 11th edition edition, 2014.

[145] D. Verdon and G. McGraw. Risk analysis in software design. *IEEE Security and Privacy*, 2(4):79–84, 2004.

[146] R. von Solms and J. V. Niekerk. From information security to cyber security. *Computers & Security*, 38:97–102, 2013.

[147] A. R. Willis. Business insurance: First-party commercial property insurance and the physical damage requirement in a computer-dominated world. *Florida State University Law Review*, 37(4), 2010.

[148] Z. Yang and J. C. S. Lui. Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, 74:1–17, Apr. 2014.

[149] W. Yurcik and D. Doss. Cyberinsurance: A market solution to the internet security market failure. In *Proceedings of the 1-st Workshop on the Economics of Information Security*, 2002.

[150] X. Zhao, L. Xue, and A. B. Whinston. Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling. In *Proceedings of the International Conference on Information Systems, ICIS 2009, Phoenix, Arizona, USA, December 15-18, 2009*, page 49, 2009.