ARTICLE IN PRESS

Computer Science Review ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Survey

Cyber-insurance survey[☆]

Angelica Marotta [b], Fabio Martinelli [b], Stefano Nanni [a], Albina Orlando [c], Artsiom Yautsiukhin [b,*]

[a] Unipol Gruppo Finanziario S.p.A., Bologna, Italy

[b] Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy

[c] Instituto per le Applicazioni del Calcolo "Mauro Picone", Consiglio Nazionale delle Ricerche, Naples, Italy

HIGHLIGHTS

- Discussed a number of peculiarities of cyber insurance.
- Provided necessary formal background.
- Reviewed available literature on the topic.
- Analysed applicability of cyber insurance in the main technological systems.
- Listed a number of possible research directions in the topic of cyber insurance.

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Cyber insurance
Security
Risk management

ABSTRACT

Cyber insurance is a rapidly developing area which draws more and more attention of practitioners and researchers. Insurance, an alternative way to deal with residual risks, was only recently applied to the 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.

© 2017 Elsevier Inc. All rights reserved.

Contents

1. Introduction 3
   1.1. Motivation 3
   1.2. Contribution 3
   1.3. Structure of the paper 4
2. Market solutions for cyber-insurance 4
   2.1. Past of cyber insurance market 4
   2.2. Current cyber insurance market status 4
      2.2.1. Cyber insurance domains 4
      2.2.2. Security coverage 4
      2.2.3. Privacy coverage 5

☆ This work was partially supported by projects H2020 MSCA NeCS 675320 and H2020 MSCA CyberSure 734815.

* Corresponding author.
E-mail addresses: angelica.marotta@iit.cnr.it (A. Marotta), fabio.martinelli@iit.cnr.it (F. Martinelli), Stefano.Nanni@unipolsai.it (S. Nanni), A.Orlando@na.iac.cnr.it (A. Orlando), artsiom.yautsiukhin@iit.cnr.it (A. Yautsiukhin).

http://dx.doi.org/10.1016/j.cosrev.2017.01.001
1574-0137/© 2017 Elsevier Inc. All rights reserved.

2.2.4. Agent attitude to cyber insurance ... 5
2.3. Future of the cyber insurance market ... 5
2.3.1. USA ... 5
2.3.2. Europe ... 5
3. Basic definitions ... 5
3.1. Actors ... 5
3.2. Risk management ... 5
3.3. Insurance contract ... 6
3.4. Insurance process ... 6
4. Cyber-insurance ... 6
4.1. Peculiarities of cyber-insurance ... 6
4.1.1. Risk identification ... 6
4.1.2. Likelihood determination ... 7
4.1.3. Impact determination ... 7
4.1.4. Risk estimation ... 7
4.1.5. Coverage specification ... 7
4.1.6. Premium estimation ... 7
4.1.7. Write and sign contract ... 7
4.1.8. Claim handling ... 8
4.2. Insurability of cyber risks ... 8
4.2.1. Insurability criteria by Mehr and Cammack ... 8
4.2.2. Insurability criteria by Berliner ... 8
4.2.3. Insurability analysis ... 8
5. Basic (cyber)-insurance formalisation ... 8
5.1. Utility function ... 8
5.2. Demand side. Insured ... 9
5.2.1. Expected utility without insurance ... 9
5.2.2. Expected utility with insurance ... 9
5.2.3. Self-protection ... 9
5.2.4. Multi-agent case ... 10
5.2.5. Life vs. non-life insurance ... 10
5.2.6. Social welfare ... 10
5.2.7. Interdependent protection ... 11
5.2.8. Insured models ... 11
5.3. Supply side. Insurer ... 11
5.3.1. Expected utility ... 11
5.3.2. Market types ... 12
5.3.3. Simple game ... 12
5.4. Environment ... 12
5.4.1. Information asymmetry ... 12
5.4.2. The game with adverse selection ... 12
5.4.3. The game with moral hazard ... 12
5.4.4. Market regulation options ... 13
6. Analysis of the literature ... 13
6.1. Risk/security level specification ... 13
6.1.1. Cyber risk management ... 13
6.1.2. Cyber risk assessment ... 13
6.1.3. Risk analysis techniques ... 14
6.2. Game theoretic approaches for premium specification ... 15
6.2.1. Independent security ... 15
6.2.2. Interdependent security ... 15
6.3. Unified approach to analysis of the literature on interdependent security ... 17
6.3.1. Definition of the unified approach ... 17
6.3.2. Competitive market ... 18
6.3.3. Non-competitive market ... 19
6.3.4. Corrective treatments ... 20
6.3.5. Summary of main findings ... 20
7. Cyber-insurance research gaps and possible directions ... 20
7.1. Analysis of technological systems ... 20
7.1.1. Insurers lack of experience and standards ... 20
7.1.2. Evolution of system ... 20
7.1.3. Information asymmetry ... 20
7.1.4. Hard to specify rate of occurrences ... 20
7.1.5. Interdependence of security ... 20
7.1.6. Lack of statistical data ... 20
7.1.7. Hard to estimate damage ... 20
7.1.8. Hard to verify ... 21
7.1.9. Unclear coverage/exclusions and limited coverage/low indemnity ... 21

Please cite this article in press as: A. Marotta, et al., Cyber-insurance survey, Computer Science Review (2017), http://dx.doi.org/10.1016/j.cosrev.2017.01.001

7.1.10. Correlated risks ... 21
7.1.11. Language/overlapping with existing insurance coverage ... 21
7.1.12. Liability ... 21
7.1.13. Time for claims ... 21
7.1.14. Forensics ... 21
7.1.15. Analysis of effects of technological systems on cyber insurance ... 21
7.2. Research gaps ... 21
7.2.1. Evolution of systems ... 21
7.2.2. Information asymmetry ... 21
7.2.3. Hard to specify rate of occurrences ... 21
7.2.4. Lack of statistical data ... 22
7.2.5. Hard to estimate damage ... 22
7.2.6. Interdependency of security ... 22
7.2.7. Correlated risks ... 22
7.2.8. Liability ... 23
8. Conclusion ... 23
References ... 23

1. Introduction

In recent years, there has been a growing interest to cyber risk and it is considered among the most challenging issues to deal with, as cyber risk could lead to serious impact on businesses and societies [1]. 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 [2–5]. Many companies are starting to consider cyber security as a large business risk and, as a consequence, they are looking for methods to ensure the continuity of financial operations in case of cyber attacks [6].

In spite of the wide application of security measures, the losses due to breaches are still extremely high [7]. The study of cyber risk conducted by Marsh in 2013 revealed that 54% of the interviewed organisations have been subject of a cyber attack in the last 3 years (when 17% of respondents were not able to answer the question). Furthermore, according to the study commissioned and managed by European Network and Information Security Agency (ENISA) [8], the average cost per breach based on data from underwriters was US$2.4m. Research conducted by Ponemon Institute [6] revealed that the average financial impact to companies due to cyber incidents was $9.4 million. The average cost per a compromised record is assessed to be $188 according to Ponemon Institute [6] or $107.14 according to NetDiligence [9]. These examples show that it is impossible to completely mitigate cyber risks, while the possible impact becomes larger with higher dependence of business and society on information technologies. Although there is no doubts that since security countermeasures and practices are important, risk managers should also look for other options to deal with residual cyber risks.

One of the alternatives in dealing with residual risks is risk transfer, which usually means insurance [10–15]. Starting since 1998 [16–18] cyber insurance policies became more and more popular on the market [19]. Global surveys [1,20] and books [21] on insurance consider cyber risks as an important component of risk management programs. More than 50 insurers now provide cyber insurance policies from US, Bermuda and London markets [22,23]. The gross written premium in US is predicted to be 2,75 billion in 2015 [24] and 150 million in Europe, rising from 50 to 100% annually (prediction for 2014) [25].

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 positive effect. First and the foremost advantage of insurance is the possibility to provoke organisations to increase investments in their protection, in order to reduce the premium [10,18,26–30]. Next, cyber insurance is believed to improve the societal welfare by improving the overall level of cyber protection [18]. Third, cyber insurance (premiums, in particular) may serve as an indicator of quality of protection [10,27,31,32]. Last but not least, cyber insurance may lead to new and more advanced standards in cyber security [8,19,30], since adherence to security standards or possessing a certificate may be the simplest way for a cyber insurer to estimate the risk exposure of insured.

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 different pricing and regulatory strategies on the market [14, 33–41]. The primary focus of researchers is on the issue of interdependency of security, one of the peculiarities of cyber risks.

1.1. Motivation

In the past, there were several comprehensive studies, which, although were not called "surveys", provided extensive analysis of the available literature and marketing practices for the time when they were released. R. Majuca et al. [18] presented an overview on evolution of cyber insurance by 2005. The study was mostly focused on the market analysis and provided a high level discussion of basic problems (e.g., moral hazard). R. Böhme and G. Schwartz [42] proposed a unified approach for cyber insurance in 2010, glueing together different aspects of cyber insurance and indicating the approaches of different researchers dealing with these aspects. In sum, regardless the raising importance of cyber insurance and increasing number of related scientific publications, there is no a comprehensive survey on the topic.

1.2. Contribution

In contrast to existing works, the primary focus of this paper is on *surveying* the existing literature on cyber insurance. We provide a different approach to summarising the results with the most up-to-date and comprehensive review of the literature. To our knowledge, this is the first attempt to summarise the dispersed results on the topic under the same umbrella. This unified approach helped us to find the situations, where authors came to the same conclusions and where authors disagree and further research is required.

In this work, we summarise various results achieved in cyber insurance so far and outline future 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. In the paper we provide a baseline mathematical model and explain formalisation of basic concepts. We do not have a goal to provide a comprehensive tutorial, but we

would like to help readers to understand the core concepts, which are usually only briefly mentioned in the dedicated articles. Finally, out of our insurability analysis of different modern technological domains (and findings of various authors) we draw a number of future directions for scientific and practical improvements in the area of cyber insurance.

1.3. Structure of the paper

The paper is organised as follows. We report brief history, outline the current practices and sketch future predictions for the cyber insurance market in Section 2. Then, the survey summarises the background information on cyber insurance, in order to introduce readers into the basic terms and process (see Section 3). After that we discuss the peculiarities of cyber insurance, as one of many applications of insurance (see Section 4). Before going into the analysis of scientific papers on cyber insurance, we define a baseline mathematical model (see Section 5). The core analysis of the available approaches is performed in Section 6. First, we outline various practices available for risk assessment and show how they can be applied in the cyber insurance process (see Section 6.1). Then, we go deeper into cyber insurance approaches, highlighting the main scientific directions and achievements in the field (see Section 6.2). Finally, we devote a special attention to the main problems considered in the scientific literature, e.g., whether cyber insurance may serve as an incentive for increasing self-protection, by comparing different studies in a unique, structured way (see Section 6.3). Finally, we consider different technological domains, taking into account the most recent advances in information technologies, and analyse the possibility to apply cyber insurance to them (see Section 7.1). We conclude the paper with highlighting identified research gaps for further research (Section 7.2) and a short summary (Section 8).

2. 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 practices and finish the section with the predictions made by leading cyber insurers and analysts.

2.1. Past of cyber insurance market

Specialised coverage against computer crime first appeared in the late 1970s [18]. In 1990, insurance policies as packages (software + insurance) started to be offered by security software companies partnering with insurance companies [36]. In 1998, the earliest known separate hacker insurance policies were first introduced by the International Computer Security Association (ICSA Inc.). This organisation offered insurance against hacker attacks as a part of its TruSecure service [16–18]. Since that time, the stand-alone cyber insurance market has grown up to 50 or 60 insurers from US, Bermuda and London markets [22,23].

One of the main drivers for cyber insurance market is severe cyber events occurring within major companies that caused big losses. For example, in February 2000, hackers launched 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 [5]. Companies that experienced these disasters became much more interested in purchasing cyber insurance policies to mitigate future losses [6,19,43] and more insurance companies developed the corresponding products to satisfy this need [44]. 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 complexity of information systems.

Regulations on data protection are another strong driver for cyber insurance market. In 2003, the amount of introduced cyber insurance policies grew significantly in US [45] as a results of California data breach notification law [46] being passed. This law required a state agency, 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 48 US state legislatures and there are moves to implement a national notification standard concerning compromised data [47, 48]. Since then other countries started considering the possibility to introduce similar laws (e.g., Canada, Australia [48]). In January 2012, the European Commission unveiled its draft data protection Regulation, intended to update and harmonise the EU data protection law [49,50]. According to the European Parliament legislative resolution on 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 h (this time has been changed to 72 h after the first reading [49]).

2.2. Current cyber insurance market status

In a survey conducted by ACE in 2012 [51], 99% of 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.

2.2.1. Cyber insurance domains

According to the 2014 Batterley Risk Report [52], now market trends seem to increase, especially in healthcare and the small- to mid-sized segments. For example, Chubb already provides a product called Cyber Security for Healthcare Organizations that offers coverage for cyber risks related to the medical field [53]. In fact, out of 145 data breach insurance claims analysed in the report of NetDiligence [9], the healthcare was the sector most frequently breached (29.3%). Other market sectors interested in cyber insurance are professional services, financial services, information technology, the retail sector, etc. [54]. The most commonly exposed data are PII (personally identifiable information) and PHI (private health information) [9,19].

2.2.2. Security coverage

Insurance companies develop two different types of cyber insurance (First-party and Third-party) in order to meet the cyber needs of both company that work in IT and other types of companies. Table 1 represents an overview of what type of coverage is currently offered on the market. In particular, Table 1 proposes a comparison between the top insurance companies offering cyber insurance coverage such as Allianz, Zurich, Marsh, etc. For every company, we put $\times$ if the provided policy covers the losses. We mark the cell with $\times^*$ if a more in-depth protection plan is available (for a higher premium), which covers the losses not covered by the standard version of the policy.

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 available indemnity ranges from

Table 1
Coverage of several existing insurance policies.

	Coverage	Allianz [55]	QBE [56]	AEGIS [57]	CNA [58]	InsureTrust [59]	CDRM LLC [60]	Travelers [61]	Zurich [62]	ACE [63]	Hiscox [64]	Insureon [65]	Marsh [66]	Chubb [67]	AIG [68]
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 forensics investigation	×	×	×*	×	×	×			×		×			×
	Customer notification/PR expenses	×	×		×	×	×	×	×	×		×		×	×
	Multi-media liability	×	×	×		×		×	×*	×					×
	Loss of third-party data	×*		×	×*	×	×	×	×	×	×	×	×	×	
	Third-party contractual indemnification		×			×			×	×				×	

10 millions up to 100 millions depending on the selected packages [55].

Additionally, some policies next to the damage coverage, offer prompt support in case of a loss, or other cyber events through the assistance of specialised 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 [56]).

2.2.3. Privacy coverage

Particular attention is given to privacy. Privacy coverage is clearly driving the market [52]. For example, the company ACE has a specific product called ACE Privacy Protection® [63] which provides specific coverage up to $20 million and focuses on privacy liability.

2.2.4. 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 [69], 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 [70]: 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 have declared to be satisfied [6].

2.3. Future of the cyber insurance market

2.3.1. 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) [42,71]. 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 [52] revealed, that the gross premiums for cyber-insurance in US in 2014 was 2.0 billions (and was 1.3 billion, in 2013) growing 10%–25% per year, that coincides with the predictions of Marsh & McLennan Co [25]. The most recent report [24] has shown that the annual gross written premium could be around 2,75 billions in 2015.

2.3.2. Europe

In Europe, the cyber insurance market is growing as well. As reported by the Fourth Annual Survey of Enterprise-Wide Cyber Risk Management Practices in Europe conducted by Advisen [69], while the European cyber insurance market is still significantly below the levels seen in the US, (the European market is estimated to be less than $150 million) it is rising by 50%–100% annually, according to Marsh [25]. Thus, the cyber insurance market in Europe is a great opportunity with high potential and low competition.

3. 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 alternative for 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 establishing and claim handling. We conclude the section with a specification of a cyber-insurance process.

3.1. Actors

We start with the definition of 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, while the insured is a demand side. In this paper we use also the term *agent* to refer to a party that potentially can buy an insurance policy, but it is irrelevant for the consideration whether it actually has already bought the policy or has not. The insurance process also may involve other parties like a *verifier*, a *consultancy agency*, *police*, etc., which are self-explanatory.

3.2. Risk management

Insurance is a way to manage risks. Moreover, the idea of risk management has been originated and generalised from insurance management [21]. Thus, in order to understand insurance we should define risk management first.

Risk is the possibility of suffering harm or loss [72]. 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 *incident*. This possibility of risk occurrence depends on two aspects: threat and vulnerability. A *threat* specifies the cause of risk (fire, kidnapping, leakage of confidential information, etc.).

A *vulnerability* is an existing flaw or weakness, which can be exploited and result in an incident.

Second, the definition of risk states that risk may result in losses for an agent. Losses occur because of the consequences of incidents, 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 secret information, a business goal [73], etc.

Thus, a risk exists only if there are a cause, a possibility and a consequence of an incident. 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 [72]. 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 incident and the amount of impact of the incident, and can be seen as:

$$Risk = Probability \times Impact. \quad (1)$$

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

Risk treatment is a sub-process for selecting and implementing measures to deal with risks. There are four alternatives: risk mitigation (or risk reduction), risk transfer, risk avoidance, and risk acceptance. *Risk mitigation* consists of 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 a risky event (e.g., withdraw from a risky part of business). *Risk acceptance* is simple acknowledgement that the estimated losses may take place. Naturally, risk acceptance is automatically applied without any decision explicitly taken.

3.3. 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 an insured to an insurer for assuming the risk. *Exclusions* are the risks excluded from an insurance policy. *Coverage* is the amount of risk or liability covered by an 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 by insurance: the *first-party* coverage insure against the losses for the insured itself, while the *third-party* coverage covers the damage to third parties. An example could be a fire insurance policy, which, in case of an incident, 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 incident occurs, the insured activates the insurance policy by sending a *claim* to the 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, while secondary losses are indirect ones. Examples of secondary losses are losses to the reputation or decrease in stock market.

3.4. Insurance process

In general, the process for cyber insurance could be seen as follows. First, an evaluator 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 incident and aggregating these values. Usually, the next phase is risk treatment [74–76], but since the focus of this survey is on insurance, w.l.o.g., we assume, that the risk transfer option is selected. Then, the agent and the insurer specify coverage and the premium. After signing the contract, and in case an incident has occurred during the contractual period, the agent may make a claim to the insurer to cover the losses. In short, the process could be seen as follows:

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. Establish Contract
   (a) Coverage Specification.
   (b) Premium Estimation.
   (c) Write and Sign Contract.
   (d) Claim Handling (optional).

Here we focus more on the problem of insurance contract underwriting, and only briefly mention the following (optional) actions, which are grouped as Claim Handling. We do this because the majority of the steps, which are specific for cyber insurance, belong to the underwriting process, when only a few issues are specific for Claim Handling, as we will show in the following.

Ideally, the process is performed by both an insured and an insurer, taking into account the needs of and means available to each party. An agent first performs Phases 1 and 2 and decides whether insurance is a suitable option for it as a treatment. Then, the insurer performs a similar analysis (often with a much simplified process, e.g., by means of a standard questionnaire and profiling the agent). An insurer is not usually involved in risk treatment for the agent, but it may suggest or demand implementation of security countermeasures, which affect the premium [10,19,77]. Finally, Phase 3 is a collaborative sub-process, although both parties tend to shift the contract in their favour.

4. Cyber-insurance

This section is devoted to the key peculiarities of cyber insurance with respect to insurance in general. In this section we list these peculiarities and provide the insurability analysis of cyber insurance to show whether insurance is applicable to cyber risks and how the found peculiarities affect the insurability criteria.

4.1. Peculiarities of cyber-insurance

Here we summarise the main issues related to the application of insurance to cyber security. We group the issues by the steps of insurance process (see Section 3.4).

4.1.1. 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 [18,26,29,52,78].

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 [8,23,79,80].

4.1.2. 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 [8,11,12,23,26,81–84]. 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 [27]. Furthermore, it is easy to install protective software (e.g., a firewall, antivirus) and poorly maintain them [29]. Finally, insurers should not forget that security is a process, not a product [38,79,85].

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 [7,79]. Although the determination of rates of occurrences itself is a hard task (see, for example, papers on security evaluation, like [86,87]), several reasons make it even harder:

Evolution of attacks —techniques used by attackers are constantly changing. New attacks come to play, while old ones vanish. The attackers are highly adaptable and changes are very unpredictable [47,52,80,82,88–90].

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 insurers to define the requirements for reducing premiums [8,14,26,91].

Interdependence of security. Security level of one system (may) depends on security of others [8,10,18,26,38,42,47,80–82,92]. For example, a virus may penetrate into a system through a channel established with a partner (with much weaker security). 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 [8,10,11,18,23,26,47,82,83,90,93,94] information on cyber threat incidents 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 they cause large (often, not covered) secondary damage, e.g., to reputation [23,29,83,95]. There is no publicly available comprehensive and consistent database of breaches [12]. For example, Biener et al. [82] 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.

4.1.3. 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 [8,10,11,23,26,80,83,95,96]. 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 a large portion of the whole damage is very difficult to estimate.

4.1.4. Risk estimation

Hard to verify. It is currently almost impossible to verify correctness of the estimated risks [86].

4.1.5. 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 [8,82,91,97]. This issue is particularly hard with the dynamicity of threats.

Exclusions and limited coverage. Current policies contain a lot of exclusions [6,29,43] and are limited in coverage [6,23,26,38,52,70].

Low indemnity limits. The indemnity limits are too small (max 100 millions) for large corporations.

4.1.6. Premium estimation

Correlated risks. Risk threatening one insured may also correlate with risk for another insured. Examples: worms, similar bugs, etc. [8,10,12,23,26,31,52,81,90]. 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 [8,26,29,42,82]. Although currently there are few re-insurers for cyber risks, there is a tendency for such actors to become more and more interested in cyber risks [24].

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., [82] 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 [10,13,14,42,52].

Easy to perform —attacks are easy and cheap to perform. The adversary may attack from any place in the world. Moreover, it is extremely hard to track them down, and, consequently, to punish. Many organisations do not even notify police about the breaches [11,98]. 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. 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 [29,52,99].

Overlapping with existing insurance coverage. Companies think that they do not need cyber insurance since their general insurance package already covers their needs [8,23,79,89].

Liability. When a cyber incident occurs it is necessary to establish the responsibility for the damage and define who is responsible for the losses. In the digital world this is not always clear [10,12–14,23,26,29,89,91,98]. 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 [23].

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 [80,100].

Forensics. The insurers often require proper investigation of incidents 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 incident confidential. These secondary losses, often not covered by insurers and may prevent the agent from notifying the law enforcement agency and making a claim [14,101].

It is hard to say which of the above specified issues are the most important from the cyber insurance point of view. Naturally, the industry is more concerned of practical ones, such as lack of statistical data [10,23,47,93]. The academia is more focused on potential social function of cyber insurance (e.g., to increase the overall cyber security) and, thus, looks for methods to overcome interdependent security and information asymmetry issues [35–37,39,81,102–104].

4.2. Insurability of cyber risks

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

4.2.1. Insurability criteria by Mehr and Cammack

R. Mehr and E. Cammack [105] formulated seven requisites of insurable risk:

Incidental loss. The incident 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 incident.
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 for 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 itself.

4.2.2. Insurability criteria by Berliner

R. Berliner [82,106] formulated nine criteria of insurable risk (the first five criteria refer to actuarial-mathematical model, sixth and seventh to the market conditions, and last two to environment):

Randomness of loss occurrence incidents must happen independently.
Maximum possible loss per incident should be manageable for insurer.
Average loss per incident should be moderate.
Loss exposure should be large enough.
Information asymmetry should not 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.

4.2.3. Insurability analysis

Several studies [8,82,107] analysed cyber risks according to these criteria of insurability. They have found that, although cyber risk has some problems with satisfying several criteria, in general, cyber risk can be insured, although more work needs to be done to make the market more mature.

We have collected the results of the studies in Table 2. We colour the criteria found to be non-problematic in white, moderately problematic—in light grey 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 2). Also the importance of the large information asymmetry issue can be seen in the amount of the scientific papers on the matter (see Section 6). As for randomness of loss occurrences, then here the conclusions of the informal analysis of ENISA [8] and C. Biener et al. [82,107] 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. Basic (cyber)-insurance formalisation

This section introduces the basics of the mathematical modelling tools for cyber insurance. Here we introduce many concepts from general insurance theory to help cyber security researchers to get basics of the applied mathematical models. The issues related to cyber insurance are mostly captured by interdependent security and topology models.

5.1. Utility function

A starting point is the concept of "utility". Utility is a term used by economists indicating the satisfaction a consumer receives from a product. Such approach leads to differentiation of the amount of wealth and the utility that the wealth provides.

Let $\boldsymbol{W}$ be a random variable denoting the amount of wealth of an agent in a considered situation. Let W^0 be a fixed value of the initial wealth of an agent. In the following, we denote all random variables as bold, while concrete values are not bold.

Let us consider a generic utility function $U(\boldsymbol{W})$, which returns the utility for a specific amount of wealth for an agent. This function is a von Neumann–Morgenstern utility function, which correctly represents[1] the expected outcome in a game with two possible outcomes (e.g., bad and good ones). The exact form of the utility function 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. Mathematically, this means that the utility function is assumed to be twice deferential and concave: $U'(\boldsymbol{W}) > 0$ and $U''(\boldsymbol{W}) < 0$. The first inequality requires the agent to prefer more wealth to less (avidity); the second inequality requires that the value it puts on a given increment in wealth decreases as the level of wealth increases (risk aversion).

[1] We refer the interested reader to the original book of J. von Neumann and O. Morgenstern [108] for the precise specification of the conditions/axioms for rational choice of an agent and a formal proof that an expected utility correctly represents the values for the choice.

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

Phases	Steps	Criteria of [106,107,82]	Criteria of [105,8]	Open issues
Risk identification	Asset identification			Evolution of systems Lack of experience and standards
	Threat identification			Evolution of systems Lack of experience and standards
	Security/Vulnerability identification			Evolution of systems Lack of experience and standards
Risk analysis	Likelihood determination	Loss exposure	Large number of similar exposure units	Evolution of attacks
		Randomness of loss occurrences	Incidental loss	Interdependence of security
		Information asymmetry		Information asymmetry
			Calculable loss	Hard to specify rate of occurrences Lack of statistical data
	Impact determination	Average loss per incident	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 incidents	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
	Claim handling			Time for claims Forensics

5.2. Demand side. Insured

5.2.1. Expected utility without insurance

Let a random variable $\boldsymbol{L}$ represent the individual perception of damage or injury, allowing for its likelihood. Let us consider a simple example assuming that $\boldsymbol{L}$ will be equal to 0 with probability $1-pr$ in case of no incident and will be equal to L, with probability pr, if the incident happens. The random financial position of the agent in case of no insurance option available/taken is $\boldsymbol{W}_1 = W^0 - \boldsymbol{L}$; assuming the value W^0 with probability $1-pr$ if the incident does not happen and $W^0 - L$ with probability pr, otherwise. The expected utility of the random variable $\boldsymbol{W}$ is:

$$E[U(\boldsymbol{W}_1)] = (1-pr) \times U(W^0) + pr \times U(W^0 - L). \quad (2)$$

It follows from Jensen's inequality for a concave utility function (see, for example, [109, page 62]) that

$$E[U(\boldsymbol{W}_1)] \leq U(E[\boldsymbol{W}_1]) = U(W^0 - E[\boldsymbol{L}]). \quad (3)$$

Decision makers with such utility functions prefer to pay a fixed amount $E[\boldsymbol{L}]$ instead of a risky amount $\boldsymbol{L}$, so they are risk averse.

5.2.2. Expected utility with insurance

In the case of insurance, an agent chooses between bearing an uncertain risk, which could give rise to an unknown expenditure at some point in the future, and making a definite fixed payment at the start of a policy term.

Let us suppose that an agent buys an insurance policy paying the premium P and getting an indemnity $\boldsymbol{I}$ in case of an incident. Thus, the insurance policy proposed by an insurer can be seen as a tuple: $(P, \boldsymbol{I})$. Indemnity is a random variable, since it depends on the occurred losses $\boldsymbol{L}$: $\boldsymbol{I} = f(\boldsymbol{L})$. In our initial, simplistic discussion the only possible amount of losses is L, which occurs with probability pr, then, lets $I = f(L)$ and the contract can be rewritten as (P, I).

In case of insurance the agent's random financial position is $\boldsymbol{W}_2 = W^0 - \boldsymbol{L} - P + \boldsymbol{I}$, assuming the value $W^0 - P$ with probability $1-pr$ in case of no incident and the value $W^0 - L - P + I$ with probability pr, otherwise.

Let us suppose that the insured, paying the premium P, obtains a total cover in case of loss ($\boldsymbol{I} = f(\boldsymbol{L}) = \boldsymbol{L}$). Therefore,

$$E[U(\boldsymbol{W}_2)] = U(W^0 - P). \quad (4)$$

The pure premium P is *fair* if the following relation holds:

$$P = E[\boldsymbol{I}] = E[\boldsymbol{L}]. \quad (5)$$

On the basis of Eqs. (3) and (5):

$$E[U(W^0 - \boldsymbol{L})] \leq U(W^0 - P). \quad (6)$$

Eq. (6) shows that a risk averse agent (i.e., the agent preferring paying a fixed P and having the insurer assume random loss to assuming the risk itself) will purchase insurance.[2]

The insurance contract is still convenient if the agent pays a premium $P = E[\boldsymbol{I}](1+\lambda)$ where λ is a loading term due to general expenses born out by the insurer and must be low enough to ensure that Eq. (6) holds.

5.2.3. Self-protection

An agent may invest in self-protection to reduce exposure to 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

[2] We may also see that a risk neutral agent (in case of strict equality) may want to purchase an insurance policy.

of investments in protection decreases with the increase of the protection level x.

Naturally, pr also depends on x and can be re-defined as $pr = \pi(x)$. Now, the random financial position of the agent in case of no insurance is $W_2 = W^0 - \boldsymbol{L} - C(x)$, while with insurance its value is $\boldsymbol{W}^I = W^0 - \boldsymbol{L} - C(x) - P + \boldsymbol{I}$.

Now, we write the expected utility in both cases:

with insurance :

$$E[U(\boldsymbol{W}^I)] = (1 - \pi(x)) \times U(W^0 - P - C(x)) + \pi(x) \times U(W^0 - L - P + I - C(x)). \quad (7)$$

without insurance :

$$E[U(\boldsymbol{W}^N)] = (1 - \pi(x)) \times U(W^0 - C(x)) + \pi(x) \times U(W^0 - L - C(x)). \quad (8)$$

If $\boldsymbol{L} = \boldsymbol{I}$ the insurance is *full*, i.e., completely covers the losses if the threat occurs. The insurance is called *partial* if $\boldsymbol{L} > \boldsymbol{I}$. The partial insurance can be modelled as: $\boldsymbol{I} = \beta(\boldsymbol{L} - \boldsymbol{D})$, where β is a portion of losses the agent wants to be covered by and $\boldsymbol{D}$ is a deducible.

For computations we can use only Eq. (7), since Eq. (8) can be derived from Eq. (7) if the selected contract is (0,0). This contract can be received if $\beta = 0$, since a premium is usually proportional to indemnity (i.e., $P = 0$ if $I = 0$).

Thus, the agent modifies its security level x and chooses the available insurance contract (either selecting from a set of proposed contracts or specifying the portion of losses to be covered) in order to maximise its expected utility (i.e., Eq. (7)) and have it higher than the expected utility in case of no insurance: $E[U(\boldsymbol{W}^N)] < E[U(\boldsymbol{W}^I)]$.

5.2.4. Multi-agent case

Consider several agents operating in the same environment. In this more general situation pr 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*, if the probability of an incident 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 consider pr as a function $pr_i(x_i, X_{-i})$ returning the probability of an agent i to be compromised (both directly or indirectly). We refer to this function as an *incident probability function*. Naturally, if an agent may be attacked only directly, then $pr_i(x_i, X_{-i}) = pr_i(x_i)$, and is denoted as: $\pi_i(x_i)$. The incident probability function is also twice deferential and convex ($\frac{\partial pr_i}{\partial x_i} \leq 0$ and $\frac{\partial^2 pr_i}{\partial x_i^2} \geq 0$).[3]

The random financial position of the agent i in case of no insurance is $\boldsymbol{W}_i^N = W_i^0 - \boldsymbol{L}_i - C_i(x_i)$, while in case of insurance we get: $\boldsymbol{W}_i^I = W_i^0 - \boldsymbol{L}_i - P_i + \boldsymbol{I}_i - C_i(x_i)$. Referring to agent i we can rewrite the expected utility $E[U_i(\boldsymbol{W}_i)]$ as:

with insurance :

$$E[U_i(\boldsymbol{W}_i^I)] = (1 - pr_i(x_i, X_{-i})) \times U_i(W_i^0 - P_i - C_i(x_i)) + pr_i(x_i, X_{-i}) \times U_i(W_i^0 - L_i - P_i + I_i - C_i(x_i)). \quad (9)$$

without insurance :

$$E[U_i(\boldsymbol{W}_i^N)] = (1 - pr_i(x_i, X_{-i})) \times U_i(W_i^0 - C_i(x_i)) + pr_i(x_i, X_{-i}) \times U_i(W_i^0 - L_i - C_i(x_i)). \quad (10)$$

All 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 areidentical: $\forall i, j\ U_i(\boldsymbol{W}) = U_j(\boldsymbol{W}), C_i(x) = C_j(x), \pi_i(x) = \pi_j(x)$. 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 (see [110]).

5.2.5. 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, while non-life insurance is mostly related to any other type of insurance (also called causality insurance). Consequently, life insurance assumes that an incident for one insured occurs only once. The incidents covered by a non-life insurance may occur several times in a considered period. A typical period of non-life insurance is one year [79, 111,112]. Thus, in case of life insurance, it is enough to consider only the probability of occurrence (e.g., pr_i), while for non-life insurance it is required to find a rate of occurrences RO_i, i.e., a number of incident 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 pr_i instead of RO_i (with few exceptions, e.g., [113–115]). Instead, for complete non-life insurance fair premium estimation the following formula should be used: $P_i = RO_i(t)I_i$ [112].

Naturally, RO_i is a random variable by itself and can be modelled with a specific process (e.g., Poisson process or renewal process [112]). 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 by the Central Limit Theorem). The later observation underlines the practical importance of availability of genuine, complete, and representative statistical data for correct assessment.

5.2.6. 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:

$$SW = \sum_{\forall i} E[U_i(\boldsymbol{W}_i)]. \quad (11)$$

The natural goal of this regulatory entity is to maximise the Eq. (11).

[3] Note that in this case we have partial derivatives, since pr_i depends on a number of $x_j \in X$.

5.2.7. Interdependent protection

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. What makes a model more specific for cyber insurance is interdependence of protection. Although such interdependence also takes place in some other insurance cases, cyber insurance is one of the most evident examples here [10,116]. Therefore, the majority of authors consider a more complex situation when many (sometimes very large amount of [103]) 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, i.e., the security levels of agents are *interdependent*.

Let $\pi_i(x_i)$ be the probability of direct threat occurrence for an agent i, if its security level is x_i ($pr_i^{dir} = \pi_i(x_i)$). 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: $pr_i^{cont} = 1 - \prod_{j\neq i}(1 - h_{i,j} \times \pi_j(x_j))$. To find the overall probability of an incident for an agent i we should consider both events [110,35]:

$$\begin{aligned} pr_i &= 1 - (1 - pr_i^{dir})(1 - pr_i^{cont}) \\ &= 1 - (1 - \pi_i(x_i)) \times \prod_{j\neq i}(1 - h_{i,j}\pi_j(x_j)). \end{aligned} \tag{12}$$

The network is modelled with a topology model, which defines how nodes are connected. Mathematically, the topology affects the probability of contagion. In the most generic case, if a connection between two nodes does not exist this probability ($h_{i,j}$) is zero. The following specific topologies are usually considered in the literature:

- *independent nodes* [35,71,117,118]. In this case no connections exist between nodes $\forall i, j\ h_{i,j} = 0$ and they can be considered separately.

$$pr_i = \pi_i(x_i). \tag{13}$$

- *complete graph* [35,119]. In this graph every node is connected to any other node, e.g., $\forall i, j\ h_{i,j} > 0$. There are several 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 [35]:

$$pr_i = 1 - (1 - \pi_i(x_i)) \times \prod_{j\neq i}(1 - q\pi_j(x_j)). \tag{14}$$

Another case is a graph containing only *two nodes* [35,120,119]. Then, the overall probability is:

$$pr_i = 1 - (1 - \pi_i(x_i)) \times (1 - q\pi_j(x_j)). \tag{15}$$

G. Schwartz et al. [37,38,102,121] considered a complete graph representing a network of large number of agents and modelled the interdependence of security through an *average network security* value, defined as[4]:

$$\pi(\bar{x}) = 1 - \frac{1}{n}\sum_{j=1}^{n}(1 - \pi(x_j)), \tag{16}$$

$$pr_i = \pi(x_i)\pi(\bar{x}). \tag{17}$$

- *random graph (Erdös–Rényi graph)* [110,104,120]. 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).
- *weakest link security*. J. Grossklags et al., in several their studies [122–124] assumed that the probability to compromise a node could be modelled as the highest probability to compromise any node in a network. Thus,

$$pr_i = min(\pi(x_i), \pi(X_{-i})) \tag{18}$$

where abused version of $\pi(X_{-i})$ is assumed to return a set of probabilities to compromise every node in the network but i. The reverse situation, i.e., best shot security (with *max*, instead of *min* operation), is also sometimes considered by the authors, but the weakest link model is more natural and is considered in majority of authors' papers.
- *other models* [104,119,125]. Several other models could also be of potential interest, although are not frequently considered by authors: tree-shaped topology [104], star-shaped topology [119], structured clusters [125].

5.2.8. Insured models

There are two elements in the model of insured, where additional assumptions are usually made: continuity of protection levels and concrete view of utility function.

Continuity of protection levels. Protection can be considered as a continuous scale, and an agent can implement any level of protection. We will call such a model as *complete* [35,126].

Some authors consider a bit simplified, *discrete* model of insured [36,39,110,116]. In the discrete model insureds may have only one of two levels of protection: low and high. Sometimes low protection means no protection at all, in other cases high means 100% protection. Although, the levels of protection are the same, the agents usually have different cost for transition: $C_i(x_{high}) - C_i(x_{low}) \neq C_j(x_{high}) - C_j(x_{low})$ for most $i \neq j$.

Specific utility function. Since working with a *generic* version of utility is not very convenient, some authors assume a specific utility. Usual candidates here are *identity* function (risk neutral agent) [40,123]:

$$U(\boldsymbol{W}) = \boldsymbol{W}, \tag{19}$$

or a *constant absolute risk aversion* (CARA) [35,42,127–130]:

$$U(\boldsymbol{W}) = E_1 - E_2 e^{-\sigma \boldsymbol{W}}, \tag{20}$$

or *constant relative risk aversion* (CRRA) [33,42,131]:

$$U(\boldsymbol{W}) = \begin{cases} \dfrac{\boldsymbol{W}^{1-\sigma}}{1-\sigma} & \text{for } \sigma \neq 1 \\ \log(\boldsymbol{W}) & \text{for } \sigma = 1 \end{cases} \tag{21}$$

where E_1 and E_2 are positive constants and $\sigma > 0$ is a parameter of the degree of risk aversion. CARA is often applied with $E_1 = 0$ and $E_2 = 1$.

Other utility functions also could be found in the literature [132–137].

5.3. Supply side. Insurer

5.3.1. Expected utility

The insurer with utility function $U(\boldsymbol{W})$ and initial wealth W_s^0, will insure the losses paying an indemnity $\boldsymbol{I}_i$ to agent i for premium P_i if $E[U(W_s^0 + P_i - \boldsymbol{I}_i)] > U(W_s^0)$. Most papers on the studied topic

[4] The authors have re-worked their specification of the incident probability function (i.e., Eq. (17)) in [103].

consider the insurer as risk neutral. Therefore, if we consider the case of several insureds:

$$E\left[U\left(W_s^0+\sum_{\forall i}(P_i-\boldsymbol{I}_i)\right)\right]=E\left[W_s^0+\sum_{\forall i}(P_i-I_i)\right]$$
$$=W_s^0+\sum_{\forall i}(P_i-E[I_i]). \quad (22)$$

5.3.2. 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 contracts. From the mathematical perspective this means that the premiums charged by insurers are *fair premiums*, i.e., $P_i = pr_i(x_i, X_{-i}) \times I_i$. In this case, according to the Eq. (22) 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 maximisation of profit (e.g., Eq. (22)). Another important case of monopolistic market is when the monopolistic insurer is considered 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., Eq. (22) is zero).
- *Immature/Oligopoly*. 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: $P_i = (1+\lambda)pr_i(x_i, X_{-i}) \times I_i$. 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 [112]. Nevertheless, 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).

5.3.3. Simple game

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

First, the invariable values are specified[5]: W_i^0, L_i, etc. 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 (P, I) if 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 losses to be covered).

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

1. agents specify their protection levels and select the available contract types to maximise their Eq. (9);
2. the insurer instantiates the selected contracts for agents, e.g., (premium, coverage), using the protection levels of agents.

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

5.4. Environment

5.4.1. Information asymmetry

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 [85,101], but there are two cases which received a special attention.

- *Moral hazard* is a situation when a dishonest insured behaves in a way to increase the risk. Such situation is possible if 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*.
- *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 if the insurer does not have information about the probability of an incident for agents (or simply does not discriminates contracts according to the protection level). Therefore, the insurer cannot distinguish between agents with high and low risks *before signing a contract*.

The insurer in both cases is not able to compute premiums using the real probability of threat of a specific agent, but it is sometimes assumed to know the distribution of possible probabilities of threat among all agents.

5.4.2. The game with adverse selection

The adverse selection 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 [41]. 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), while 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);
2. agents select one of the proposed contract.

5.4.3. The game with moral hazard

In case of the moral hazard problem agents are free to choose a security level, while 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 [138,84].

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

1. the insurer specifies contract(s), e.g., (premium, coverage);
2. agents select the contract and specify their security levels/investments.

5.4.4. 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 threats, the model may enforce additional fines (rebates) for agents with low (correspondingly, high) protection levels. Naturally, the protection levels of agents must be known to the insurer.
- *Bonuses and penalties*. Some sort of punishment and reward may be applied when an incident has happened or not happened [139]. Although this is yet another possible regulatory option, we are aware about analysis of its effects for self-insurance only (not for general cyber insurance) [140].
- *Mandatory investments*. Some models require a minimal level of protection investments.
- *Taxes*. Additional taxes are imposed on agents with low self-protection.
- *Liability of contagion*. The agents responsible for contagion are forced to cover the caused losses.
- *Risk pooling arrangements*. This is a form of insurance where the policyholders share risk among themselves.

6. Analysis of the literature

In this section we summarise the main articles relevant for cyber insurance. To present a comprehensive picture of cyber insurance, we start with main approaches and techniques related to risk management, which are required to define possible damages and attack probabilities. Most of these approaches and techniques are topics for separate surveys. Thus, we do not go for an extensive overview of the literature here, but outline the main areas as essential for the cyber insurance process. On the other hand, we pay a specific attention to the game theoretical methods for cyber insurance and discuss the main problems studied by the authors trying to provide as extensive overview as possible. We conclude the section with our unified approach for comparison of various studies on the main problems considered by academia (e.g., whether cyber insurance is an incentive for increasing cyber protection).

6.1. Risk/security level specification

6.1.1. Cyber risk management

Risk management guidelines [76,141–143] contain generic methodologies for the risk management 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, supporting documents, and high level description of phases. Although, these guidelines often have the primary focus on the risk assessment and risk treatment phases, they also include other activities, like implementation of treatments [76,141], communication of results [142], monitoring and assessment [76,141,143], maintenance and improvement [76]. 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.

Some of the guidelines are generic and do not go deep into the risk assessment and risk treatment phases [142,143], while others go even further and next to the specific guidelines describe possible techniques [76] and even provide tools for risk assessment [141]. Moreover, the famous ISO/IEC 27001 standard [144] can also be seen as a risk management guideline since it describes all steps for risk management, including risk assessment and risk treatment.

6.1.2. Cyber risk assessment

There are a number of approaches [75,76] 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 is similar to the one defined in Section 3.4. 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 facilitate the fulfilment of specific steps.

The first revision of NIST SP 800-30 [74] 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 [141] 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) [145] and Failure mode and effects analysis (FMEA) (and its extension Failure mode, effects and criticality analysis (FMECA) [146]) are two 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 rows will specify concrete scenarios. In contrast to HAZOP, FMEA/FMECA also takes into account the probability of a scenario and its severity.

Operational Critical Treat, Assets, and Vulnerability Evaluation, OCTAVE Allegro [75], 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 [76] 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 [147–149] 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 [150]. 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 [151–155] is a framework for a 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 defencive risk analysis 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 [156] 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.

B. Karabacak and I. Sogukpinar [157] 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 answers of the interviewed persons. Then, likelihood and impact are determined as average (with respect to the amount of interviewed people) of these values. Other questionnaire-based approaches we proposed by S. P. Bennett and M. P. Kailay [158] and F. Farahmand et al. [159].

6.1.3. Risk analysis techniques

Analysis of *business documentation* [21,74,76] 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* [75,76,151]. *Questionnaires* [157], *checklists* [147–149, 159] and *worksheets* [75] can be the instruments to structure the knowledge received during such meetings, as well as filled in by the stakeholders themselves. *Delphi method* [160] 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* [74–76,147–149] 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 and provide the common practice knowledge to be re-used in concrete cases.

Threat trees [75,161], *fault trees* [74,151,162], and *attack trees* [74,76,151,163,164] are the known techniques to specify threats relevant for an agent. All these trees have a general threat as a root and then step by step make it more and more specific. Attack trees are fault trees applied in the area of cyber security. An example of an attack tree is shown in Fig. 1. The difference between attack trees and threat trees is negligible (if exists at all). A threat tree has similar ways to decompose threats per a tile (e.g., by actors, motive, outcomes), while an attack tree is more flexible and allows any kind of decomposition. *Defence trees* [165] is an extension of attack trees with possible countermeasures attached to the leaves of the tree.

History/log analysis [74,141] is the best way to determine the likelihood of an incident, assuming that the likelihood will not change in the future and statistics are 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, ISO/IEC 27001:2013 [144] 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 organisation. Other cyber security standards, which can be of interest, are: ISO/IEC 13335-1 [166], ISO/IEC 21827:2008 Systems Security Engineering—Capability Maturity Model (SSE-CMM), COBIT framework (Control Objectives for Information and related Technology) [167], IASME [168], etc. Moreover, standards for specific domains which contain security requirements also can be reused, e.g. ISO/TS 16949:2009 [169] for automotive

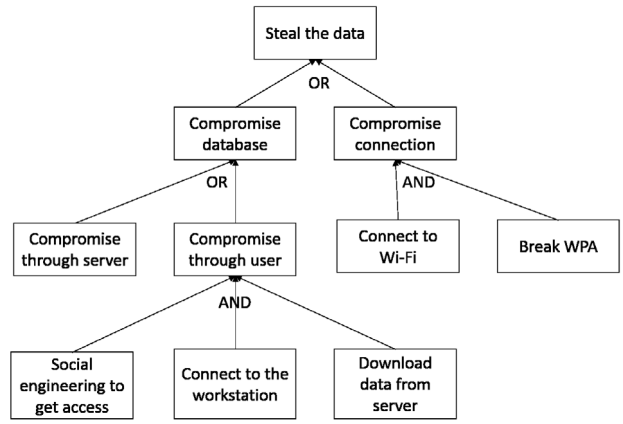

Fig. 1. An example of an attack tree.

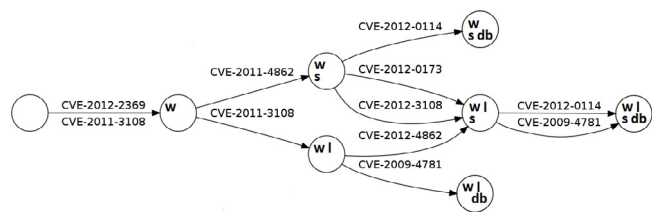

Fig. 2. An example of an attack graph.

industry, the North American Electric Reliability Corporation (NERC) Reliability Standards for Bulk Electric System (BES) [170], standard NEN 7510:2011 [171] and HIPAA for healthcare, ISO/IEC 27018:2014 [172] 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 government's Cyber Essentials Scheme [173].

Event tree analysis (ETA) [174] 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 incident and compute its probability. *Attack graphs* [175–180] 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., [181]).

An example of an attack graph can be seen in Fig. 2. We consider a simplistic attack graph for a system consisted of a workstation (w), connected to the internet, laptop (l) for maintaining the server, local server (s) with a database (db) installed on it. An analyst constructs the attack graph out of a number of vulnerabilities found in the system. Every vulnerability in the graph is represented by an arrow, which denotes the possibility for an attacker to increase its privileges in the system.

Annualised Loss Expected (ALE) [141,182] analysis and *risk tables* [74,151]. A common way to compute risk quantitatively is to use the ALE analysis. This analysis is base on Eq. (1), and uses Annualised Rate of Occurrences (ARO) (an average amount of incidents in a year) and Single Loss Expectancy (the average loss per incident):

$$ALE = ARO \times SLE. \tag{23}$$

For estimation of risks with qualitative parameters a *risk matrix* [74, 143,151] are used, which maps likelihood and impact levels to pre-defined (by experts or stakeholders) risk levels.

Profiling. In most cases, to obtain insurance, an agent simply selects one of the available insurance policies (e.g., [56,61,64,68])

and specifies the required parameters. Regarding to the answers on the questions, the insurer matches the agent against one of the pre-defined *profiles*, for which the risk and premium has already been pre-estimated. Thus, profiling helps to simplify every single underwriting process by hiding the back-office analysis, which have previously estimated the price and risk using statistical or theoretical methods, like game theory.

Game theory is a powerful mechanism for a decision making if behaviour of several participants may significantly alter the final result for everyone. We have already showed how a game may be set up for an insurance case (with and without information asymmetry problems). Both, insurer and insurer should find this analysis useful to specify the suitable indemnity and premium.[6] Moreover, for an insured, it will help to specify the most profitable portion of risks to be mitigated by countermeasures and covered by insurance. For an insurer, this analysis will help to predict its profit and effect on the society.

We summarise all these techniques in Table 3.

6.2. Game theoretic approaches for premium specification

The approaches for contract specification proposed in the literature focus on premium and indemnity estimation and mostly employ the game theory. They can be split into two sets depending on whether security of every agent is considered to be independent or interdependent. The first, the smallest, group considers various specific problems which relate to cyber insurance, while the second group is mostly focused on problems related to analysis of effect of externalities.

6.2.1. Independent security

From the high level point of view, specification of cyber risk insurance policy for a single agent does not differ much from other types of risk [98,129,183–185]. Nevertheless, several interesting problems were considered.

Secondary losses and information asymmetry. Bandyopadhyay et al. [85,101] analysed the proposed model (they used the logarithmic utility function and did not consider investments in self protection) under different scenarios (information symmetry and asymmetry) of the cyber insurance market. Particular attention of the study was devoted to secondary losses associated with a cyber incident. The results of the study show how the secondary loss exposure affects insured companies, generates information asymmetry between the insurer and the insured company, and impedes development of cyber insurance.

Cyber insurance and social welfare. Kesan et al., [71] provided an experimental method to prove that cyber insurance improves security and social welfare, if security of agents is not interdependent. R. Pal and L. Golubchik [117] analysed the problem from the perspective of an insurer: they have found that a selfish monopolistic insurer charges higher premiums to users and gets more profit with respect to a welfare-maximising insurer.

Security and non-security risks. R. Pal et al., [118] 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.

Non-life insurance. C. Barracchini and E. Addessi [113] studied contract specification for an independent agent when a threat could occur more than ones. The authors utilised a Markov chain formed by states of the system (no damage, not repairable damage and several degrees of partially repairable damage) with a possibility to restore the system to the initial state. The transition probabilities/rates are considered as given. The authors have defined two models for insurance coverage. Also S. Chaisiri et al., [114] considered a type of non-life insurance. In their model the authors assumed a risk neutral customer of a security-as-a-service provider also buying insurance. The main problem studied was the optimal allocation of expenditures by the customer to secure or/and insure arrived packets. A. Yannacopoulos et al., [115] used the random utility model for assessing the possible claimed compensation of one individual and several models for estimating the number of claims (using Poisson distribution, renewal process, mixed Poisson distribution, etc.). The union of these models allowed the authors to compute how much would an individual claim as compensation. A. Shah et al., [130] provided a simulation-based analysis using the CARA utility function and Poisson distribution of claim arrivals. The authors have shown that with increase of risk aversion of an insurer the premium rises, while with increase of risk aversion of an insured rises the percentage of bought coverage.

Attacker in the loop. Y. Hayel and Q. Zhu [186] considered a model where an attacker was considered as an active participant (and tries to maximise the damage), next to an insured and an insurer. The authors claim to consider moral hazard problem in their paper, but assume that the insurer knows the statistical distribution of investments of insureds in its portfolio. The authors investigated the conditions for an agent to engage into cyber insurance and increase its protection.

Insurance for IT outsourcing environments. S. Gritzalis et al., [128] provided a utility-based model for insuring both clients and providers of services, where the behaviour (honest or dishonest) of the providers are uncertain for clients and insurers. The authors exploited the CARA utility function and have found the conditions (the amount of fines) to force the providers to behave honestly.

6.2.2. Interdependent security

Interdependence of security is one of the most important peculiarities of cyber insurance. Since its effect on cyber insurance is not entirely known, a large number of scientific studies is devoted to this subject.

Study the effect of externalities on self-protection investments. This topic has received most attention in the scientific literature. In its essence, the topic relates to the study of effects of interdependent security on incentive of an agent to invest in self-protection in particular and on the overall protection of the society, in general. As we will show in the sequel, the problems related to the interdependent security become even more serious, when information asymmetry is in place. Here we briefly describe the most influential studies. In the following (see Section 6.3) we provide a systematic analysis of most of the studies on the topics, where the readers will be able to compare the existing approaches and their findings.

H. Ogut et al., [35] investigated the effect of interdependency of threats and immaturity of the market on security investments with cyber insurance available. The authors analysed the situation without information asymmetry and with the possibility of agents to select the amount of insurance to buy. They considered situations with competitive and non-competitive market, and of independent and interdependent security. Using a continuous model of an insured and mathematical analysis, they have come to a conclusion that security investments fall with increase of interdependency. Similar conclusions were also supported by other researchers [34,127]. Furthermore, the incentive to self-protection rises with increase of immaturity of the market (although at some point the requested coverage is reducing).

[6] In Table 3, game theory is mentioned useful for coverage specification, since it helps to estimate indemnity.

Table 3
Techniques per steps of the cyber-insurance process.

Phases	Steps	Techniques
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
Contract specification	Coverage specification	Selection by agent Meetings/interviews Game theory
	Premium estimation	Game theory Profiling
	Write & Sign policy	Paper work (digital) Signature
	Claim handling	Paper work

Finally, H. Ogut et al., considered the situation with liability for contagion and found that in this case investments in self-protection increase, they increase even higher than the social optimum level, forcing the agent to over-invest.

J. Bolot and M. Lelarge in a series of articles [36,104,119,120,187] also considered a similar problem. They applied the discrete model for insured and mathematically showed that neither competitive nor monopolistic cyber insurance market by itself can be an incentive to self-protection in case of interdependent security and information asymmetry (moral hazard). Furthermore, the authors analysed the fines and rebates treatment mechanism and have found that non-competitive and monopolistic insurers may set up their policies in such a way that insurance be an incentive to self-protection. Note, that in the later case moral hazard should be eliminated.

G. Schwartz, N. Shetty et al., [37,38,102,103,121] also analysed whether cyber insurance can be an incentive for self-protection, although these authors devoted attention to the changes of the social optimum of the self-investment level. As it has been underlined in Section 5 the authors modelled the interdependency of security through an average network security level (the ANS model). The authors devoted their attention to competitive market and considered moral hazard as well as adverse selection problems. They have found that neither for a single insured nor for the society in general cyber insurance is an incentive for self-protection. Moreover, setting an obligatory minimal investment level does not solve the problem.

Pal et al., [39] provided analysis of competitive and monopolistic markets in case of mandatory insurance applying the discrete model of insureds. In their model, an agent investing in security does not suffer from any direct, but only indirect losses. The authors have shown that competitive and monopolistic cyber insurance market without contract discrimination does not serve as an incentive for self-protection. On the other hand, monopolistic market with contract discrimination (by means of fines and rebates) could serve for such purpose, but in this case the insurer has to be able to observe investment level of agents, i.e., no information asymmetry must take place.

P. Naghizadeh and M. Liu [40] proposed an interesting variation of fines and rebates corrective treatment, which is based on the opinion of the society. Every member of the society is able to send a message, which contains its proposal on the desired public good and pricing profile. Then, the monopolistic insurer aggregates the proposals of all members and specifies a contract to enforce the socially optimal level of security. The authors have found that such scheme serves as an incentive to security only when cyber insurance is mandatory and no information asymmetry has place.

J. Grossklags et al., [188–190] performed several simulation studies to analyse the effect of interdependent security and correlated risks on predicted risk for an agent and an insurer. In particular, they have found that risks depend on the topology of the network and a cyber insurer should carefully determine the amount of required safety capital. Moreover, the authors also have shown with their simulations that it is profitable for cyber insurance providers to invest in software security to reduce correlated risks [191].

Reducing monoculture effect. Böhme [33] 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 a

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 [192] investigated similar problems. Unsurprisingly, they came to a conclusion, that cyber insurers prefer to operate in a slowly changing environment.

A provider as an insurer. S. Radosavac et al., [41] considered a model where an Internet Service Provider is also a cyber-insurer and users are able to buy an insurance from the ISP. They came to a conclusion that there is no a definitive answer whether in case of interdependency of threats the competitive market may exist. R. Pal et al., [134,135] considered a situation, where a user is able to buy a portion of security from a security provider together with insurance. The authors assume that the insurer is monopolistic and insurance is mandatory. With the use of a specific utility function and Bonacich centrality the authors have shown that it is possible to define the pricing strategy maximising the profit of the provider/insurer and convince the customers to buy some units of the self-defence product. X. Zhao et al., [34] investigated whether managed security service providers (MSSP) can also behave as an insurer. They have shown that when all agents outsource their security management to one such provider then security investment become socially optimal. F. Martinelli and A. Yautsiukhin [193] provided an approach for a service provider to willingly guarantee a reasonable level of security with additional insurance coverage. Moreover, the authors have proved that number of clients only linearly affects estimated losses per provider (and, thus, does not affect premiums per clients) even if possible attack propagation (attacking clients after compromising provider's platform) is considered.

Self-insurance and self-protection. J. Grossklags et al., devoted several studies to evaluation of the conditions for self-protection, self-insurance and market insurance. In [131], the authors considered a stand alone agent which has these three choices to mitigate its risks. No information asymmetry was considered. Moreover, the authors used a linear model for security and self-insurance investments, and assumed the CRRA utility model. They have found, that market equilibria involve full insurance coverage and is more preferable for low probability of occurrences. Finally, market insurance is more preferable than self-insurance, but is complementary to self-protection. In their following works [122, 124,194–197] the authors considered a network of agents with interdependent security (modelling the interdependency as a weakest link or as its opposite variant: best shot) and tried to investigate whether it is better for an agent to invest in self-protection or in self-insurance from both selfish and social point of view. They have found, that from the economic point of view even social optimum leads to higher self-insurance than self-protection.

6.3. Unified approach to analysis of the literature on interdependent security

In this section we provide a uniformal way to analyse the literature on effects of interdependent security on cyber insurance and security investments.

6.3.1. Definition of the unified approach

We organise diverse studies in a form of a table to analyse the papers in a unique fashion. The table has three main parts: *attributes* of the considered use case, the applied *mathematical method*, and *results*. Since, many papers apply their analysis to different situations, we split the corresponding column in as many parts as many cases were considered by the authors.

Table 4 defines the legend for attributes used in the Tables 5–7. All these attributes have been formally defined in Section 5. We did not discuss the mathematical methods for analysis because these methods are not specific for cyber insurance models, and here we mention them only to give a hint on the mathematical treatment applied by authors. Symbols (✓) and (×) for **Mandatory insurance**[7] (Section 5.4.4) and **Homogeneity** of agents (Section 5.2.4) simply state whether these attributes are considered or not.

Table 4
Legend for Tables 5–7.

Market types (Section 5.3.2)	
M	Monopolistic market
C	Competitive market
C*	Immature market
Profit of insurer (Section 5.4.4)	
ZP	Zero profit insurer
NZ	Non-zero profit insurer
max	Profit-maximising insurer
Coverage (Section 5.2.3)	
full	Full coverage
part	Partial coverage
ind	Amount of coverage is selected by insured
Information Asymmetry (Section 5.4.1)	
X	No information asymmetry
MH	Moral hazard are considered
AS	Adverse selection are considered
MH+AS	Both types are considered
Topology (Section 5.2.7)	
X	No interdependency is considered
ind	Generic model is used (Eq. (12))
Total	Complete graph
2-nodes	2 nodes graph
ANS	Average network security
ERG	Erdös–Rényi graph
Corrective treatment (Section 5.4.4)	
F/R	Fine and rebate
Tax	Additional tax
L	Liability for contagion
RPA	Risk pooling arrangements
MIL	Minimal investment level
Model of insured (Section 5.2.8)	
cont	Continuous investments
dis	Discrete investments
gen	Generic utility function
ident	Identity utility function
CARA	CARA utility function
CRRA	CRRA utility function
spec	Some specific utility function
Mathematical methods	
NE	Nash equilibrium
BNG	Bayesian Network Game
WE	Walrasian equilibrium

The main problems considered by authors could be summarised as follows:

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,

[7] Mandatory insurance is considered separately from other market regulation options for a more clear presentation, since it often complements other corrective treatments.

Table 5
Summary of approaches with competitive market model.

	Topic	Papers										
		[34]	[35]		[110]			[36]	[37]/[121]	[103]	[38]/[102]	[39]
Attributes	Market type	C	C	C	C	C	C	C	C	C	C	C
	Profit of insurer	zp	zp	zp	zp	zp	zp	zp	zp	zp	zp	zp
	Coverage full	full	ind	ind	ind	full	part	ind	ind	ind	ind	full
	Information asymmetry	×	×	×	×	MH	MH	MH	MH	MH	AS	MH+AS
	Topology	ind	×	Total	ERG	ERG	ERG	ERG	ANS	ANS	ANS	Total
	Homogeneity of agents	✓	✓	✓	×	×	×	×	✓	✓	×	×
	Mandatory insurance	×	×	×	×	×	×	×	×	×	×	×
	Corrective treatment	×	×	×	×	×	×	×	×	×	×	×
Analysis	Model of insureds	cont/gen	cont/CARA	cont/CARA	dis/gen	dis/gen	dis/gen	dis/gen	cont/gen	cont/gen	cont/gen	dis/gen
	Math. method	NE	NE	NE	BNG	BNG	BNG	NE	NE	NE	NE	WE
Results	Existence of equilibrium	✓	✓	✓	✓	×	✓	×	✓	✓	✓	✓
	Efficiency of market	–	✓	✓	✓	×	✓	–	✓	✓	✓	✓
	Incentive for self-protection	–	×	×	part	×	×	×	×	×	×	×
	Reach social optimum	×	–	×	–	–	–	–	–	✓	–	×
	Incent. social optimum	–	–	–	–	–	–	–	×	×	–	–

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

	Topic	Papers						
		[35]		[127]	[36]	[199,200]		[39]
Attributes	Market type	C*	C*	C*	M	M	M	M
	Profit of insurer	NZ	NZ	NZ	max	max	max	NZ
	Coverage full	ind	ind	ind	part	part	part	full
	Information asymmetry	×	×	×	MH	MH	AS	MH+AS
	Topology	×	Total	Total	ERG	ind	ind	Total
	Homogeneity of agents	✓	✓	✓	×	×	×	×
	Mandatory insurance	×	×	×	×	✓	✓	✓
	Corrective treatment	–	–	–	–	–	–	–
Analysis	Model of insureds	cont/CARA	cont/CARA	cont/CARA	dis/gen	dis/gen	dis/gen	dis/gen
	Math. method	NE	NE	NE	NE	BNG	BNG	NE
Results	Existence of equilibrium	✓	✓	✓	✓	✓	✓	✓
	Efficiency of market	✓	✓	✓	✓	–	–	–
	Incentive for self-protection	✓	×	×	×	–	–	×
	Reach social optimum	–	×	–	–	–	–	×
	Incent. social optimum	–	–	–	–	–	–	

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 problem is meaningless.

Incentive for self-protection —This problem checks whether the cyber insurance is an incentive for increasing investments in self-protection. In 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 (*part*)ial 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 a 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 [34].

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 the cell as (✓) if a specific result was achieved and (×) if it was not. Sometimes (part) is used to indicate that some condition should be met. 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 (Section 6.3.2). Then, we show our results for non-competitive and monopolistic markets (Section 6.3.3). Finally, we study all types of markets with applied corrective treatment (Section 6.3.4).

In short, every table shows the case studies considered in the paper (specified by the attributes) and the results derived from their mathematical analysis. The mathematical method row sheds a bit of light on the core tools the authors applied, although every study applies its own mathematical treatment. In other words, attributes define *what* has been studied, the mathematical method and model—*by what means* the analysis has been performed, while results simply report the *main findings*. This unified approach to summarise the literature should help the reader quickly identify the differences in the studies of authors and spot the conditions leading to the results.

6.3.2. Competitive market

We start with an analysis of the literature on a naive model of competitive market (Table 5). Table 5 shows that the optimal security level maximising individual utility can reach the optimal

Table 7
Summary of approaches with corrective treatment.

	Topic	Papers												
		[40]		[36]					[120,119, 187]	[35]	[39]	[34]	[37,121]	[38,102]
Attributes	Market type	M	M	M	M	M	C	C*	M	C*	M	C	C	C
	Profit of insurer	ZP	ZP	MAX	NZ	ZP	ZP	NZ	NZ	NZ	NZ	ZP	ZP	ZP
	Coverage full	ind	ind	full	full	full	full	full	full	part	full	part	full	ind
	Information asymmetry	×	×	×	×	×	×	×	×	×	×	MH	MH	AS
	Topology	ind	ind	ERG	ERG	ERG	ERG	ERG	Total	2 nodes	Total	ind	ANS	ANS
	Homogeneity of agents	×	×	×	×	×	×	×	×	✓	×	✓	✓	✓
	Mandatory insurance	✓	×	×	×	×	×	×	×	×	✓	×	×	×
	Corrective treatment	F/R	F/R	F/R	F/R	F/R	F/R	F/R+ tax	F/R	L	F/R	RPA	MIL	MIL
Analysis	Model of insureds	dis/ident	dis/ident	dis/gen	dis/gen	dis/gen	dis/gen	dis/gen	dis/gen	cont/CARA	dis/gen	cont/spec	cont/gen	cont/gen
	Math. method	NE	NE	NE	NE	NE	NE	NE	NE	NE	NE	NE	NE	NE
Results	Existence of equilibrium	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	×
	Efficiency of market	–	×	✓	✓	✓	–	✓	✓	✓	–	✓	✓	–
	Incentive for self-protection	✓	×	×	✓	✓	×	✓	✓	–	✓	×	×	–
	Reach social optimum	✓	×	–	–	–	–	–	–	×	✓	–	×	–
	Incent. social optimum	–	–	–	–	–	–	–	–	–	–	–	–	–

security level maximising social welfare only if a complete symmetry exists between agents [103]. On the other hand, H. Ogut et al., [35] with similar pre-conditions came to opposite conclusions. One possibility for this contradiction could be a slightly different topology 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., [110] show both formally and empirically that security could be an incentive for security investments if specified conditions are satisfied. In contrast, Ogut et al., [35] came to a conclusion that under the same conditions 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., [110] considered discrete model for security investments (i.e., an agent may either invest into security or not), while Ogut et al., [35] 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 topologies: random graphs result in different effects on interdependency for agents. The third explanation could be the assumption made by Ogut et al., [35] that possible losses are much smaller that the initial wealth. This assumption contradicts to the conditions specified by I. Ehrlich and G. S. Becker [198] for insurance to be incentive for self-protection.

Finally, Yang et al., [110] and M. Lelarge and J. Bolot [36] contradict to N. Shetty et al., [37,121] in the possibility for the equilibrium to exist for similar cases. One possible explanation for the fact that N. Shetty et al., [37,121] were able to find an equilibrium could be that in their work the authors consider homogeneous agents affected through average network security (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 [36] considered heterogeneous agents (with different effects of investments on self-protection), and Yang et al., [110] also used a random graph as a model of the network topology, rather than a symmetric total graph.

6.3.3. 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 in case 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 5.2.7). We summarised the main findings for the immature market in Table 6.

We see that these types of market have received less attention by the authors. A few studies suggested that the immature market is also not a good incentive for self-protection [36,39] and that the optimal values do not maximise the social welfare [35,39]. Even the mandatory insurance does not improve the situation [39,199,200]. Probably, this inability to solve these problems forced the authors to devote more attention to application of different corrective treatments in context of these markets. Nevertheless, here we may 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 [35,36,39,199,200].

It is important to note, that although the pre-conditions in Table 6 for H. Ogut et al. [35] and W. Shim [127] are similar, the later paper also provides a study of 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., [34]). W.

Shim [127] has shown that 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.

6.3.4. Corrective treatments

We saw that for all types of market, in contrast to opinions of security researchers [18,26–29], 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 summarised in Table 7.

First of all we see that using fines and rebates (F/R) 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 if no information asymmetry is in place, since the insurer has to be able to observe the security protection of agents. Furthermore, the results show that an insurer should not maximise its profit [36] (although non-zero profit is possible [36,119,120,187]). 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 if the insurer has zero profit [36]. In the later case, the insurer only re-distributes the money from low security agents to the agents with higher security [36,39,40]. We see that it is not clear from the available studies whether mandatory insurance is required for operation of this mechanism [39,40,134,135] or it is not [36,119,120,187].

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 [37,38,121,102]. 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 [34].

6.3.5. Summary of main findings

In short, we may summarise 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 exists.**
- **It is unclear whether insurance can be served as a tool for approaching optimal level of investments. Some studies contradict on this point.**
- **Effect of heterogeneity of nodes and validity of the discrete model of insureds needs a more focused study.**

7. Cyber-insurance research gaps and possible directions

In this section, we a analyse insurability of various technological systems and outline research gaps and possible directions for cyber insurance research.

7.1. Analysis of technological systems

We have already mentioned the main issues for cyber-insurance (see Section 4.1). *These issues are relevant for any technological systems for which insurance can be applied, but the extent to which the cyber insurance is affected depends on the technology used by the insured*. In this section we are going to consider how relevant the issues for specific technological systems are, i.e., how much attention should be devoted to specific problems by the insurance carrier, while a business using one of the considered systems is to be insured. The considered technological systems may sometimes overlap (e.g., mobile devices may be a part of an SME), but we consider them separately, to focus on the analysis of their distinct characteristics.

First, we list the technological characteristics contributing to the issues of cyber insurance (identified in Section 4.1). Sometimes, the cause for issues is simply "lack of experience". Since this cause is not grounded in technology, but in the immaturity of cyber insurance market, we do not consider such cause in the following analysis of technological systems.

7.1.1. Insurers lack of experience and standards

This issue is related to `lack of experience`, rather than to a characteristic of a technological system.

7.1.2. Evolution of system

Systems evolve due to two reasons: `dynamicity of the system` itself and `evolution of technology`. In the first case, it is the internal structure of the system that changes. In the second case, rapid evolution of technology and its application is a problem for insurance.

7.1.3. Information asymmetry

The technological characteristics which contribute to information asymmetry are: `''closure'' of security system` and `easiness to change controls`. First, if information about security is not available to a carrier, effective pricing is problematic (adverse selection problem). Also, if it is easy to change controls unnoticed, the insurer has to be extra careful to be sure that initial assumptions about security of the system are correct also during the contract period (moral hazard problem).

7.1.4. Hard to specify rate of occurrences

Here we also single out two characteristics directly related to the sub-issues stated in Section 4.1. First, fast `evolution of threats` is one obstacle to reliable collection of statistics. Second, effectiveness of controls often `depends on the correct operation` of these controls. In other words, it is not enough to install a control, but it is often more important to use this control correctly.

7.1.5. Interdependence of security

Two types of interdependence is important: internal and external [33]. `Internal interdependence` means that units inside a system are heavily coherent, while high `external interdependence` states that a system is connected with many other systems, out of its control.

7.1.6. Lack of statistical data

Although this issue much depends on simple lack of experience of cyber insurers, the lack of statistical evidence also can be explained by the `possibility to keep evidences of an occurred incident hidden`. Another important issue that affects representative collection of statistical data is `scarcity of similar systems`.

7.1.7. Hard to estimate damage

The first problem with estimation of damage for cyber risks is that a large part of its impact is intangible. Thus, we would like to consider a portion of possible `intangible impact` with respect to tangible one. Second, the exact impact of an event may vary significantly. Such `unpredictable impact` impedes the precise pricing.

7.1.8. Hard to verify

This issue is related to general `lack of experience` in cyber risk management.

7.1.9. Unclear coverage/exclusions and limited coverage/low indemnity

These issues are related to general `lack of experience` in cyber insurance policy writing and low maturity of the market itself.

7.1.10. Correlated risks

Lack of re-insurance can be considered simply as a consequence of `lack of experience` of cyber insurance market. On the other hand, `geographical similarity`, `Monoculture` and `possibility to replicate attacks`, affecting many system across the world in a short amount of time—can be seen as the characteristics of technologies.

7.1.11. Language/overlapping with existing insurance coverage

These issues again are related to general `lack of experience` in cyber insurance policy writing practices.

7.1.12. Liability

`Additional liability` does not primarily derive from the technology, but from its application. Thus, we try to analyse where application of considered technology systems usually leads to the issue of additional liability.

7.1.13. Time for claims

Some `threats may occur unnoticed`, and the damage may happen long after the successful penetration. An attacker may start using the database of stolen credit cards months after the attack. Whether and when such threats should be covered is mostly the problem for correct policy writing, and here we consider only the possibility of such event.

7.1.14. Forensics

The problem with forensics we refer to the `lack of experience` in policy writing and complete specification of the damage covered.

7.1.15. Analysis of effects of technological systems on cyber insurance

We summarise the main peculiarities of the technological systems with respect to cyber insurance issues in Table 8. One of the conclusions we can make out of the table is that various providers (ISP, Cloud, Social Networks) and enterprises (SME and Big enterprises) are the most problematic from the cyber insurance point of view. The main problems are: the dynamicity of the systems, difficulty to know exactly the installed countermeasures, unpredictable impact, high interdependence and additional liability.

Single devices, related to workstations and mobile devices owned by individuals and networks of devices are a bit less problematic. The advantage of single devices from the cyber insurance point of view is their multiplicity, which allows quick collection of required statistics, and low additional liability. High similarity between devices also contributes to collection of the required statistics and helps to determine possible impact more precisely. On the other hand, multitude of low value insureds will probably mean that control over the declared protection may be too costly to install. Also, similarity of systems lead to high probability of simultaneous attacks (e.g., by a new virus). Finally, lack of experience will most probably lead to poor management of installed countermeasures and high level of undetected attacks.

Network of devices have a quite wide application and many characteristics are hard to specify without relation to a concrete case. Precise specification of functionalities of the united devices or sensors will lead to more precise determination of possible damage. Moreover, the external dependency of such systems is relatively low. One issue, though, which can be a problem here is the dynamicity of the networks.

Finally, specific systems (cyber–physical and industrial systems) are less affected by usual problems of cyber insurance. These are reliable, long-living, unique systems. On the other hand, there are some serious issues as well: closure of the system and possibility to keep incidents secret. Many of these systems provide basic functionalities on local and country levels (e.g., power and water provisioning), may have desirous consequences (e.g., nuclear plants or gas and oil industry) or used in situations where human lives can be threatened (e.g., cars or medical devices). Finally, not only does uniqueness of systems reduce the possibility of cyber hurricanes, but it also hardens the collection of statistics.

7.2. Research gaps

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 (and distilled in Section 7.1).

7.2.1. Evolution of systems

Dynamic cyber-insurance. Many domains analysed in Table 8 assume that environment is dynamic; this is especially related to providers of different services. This dynamicity has an effect on the computation of the probability of an incident and increases the difficulty of assessment and re-assessment of systems, 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.

7.2.2. Information asymmetry

New solutions. The analysis of the literature in Section 6.2 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 platforms.

7.2.3. 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 [86,201] affect the rate of occurrences and can be used to specify a security level [202,203].

Table 8
Impact of characteristics of technical systems on cyber insurance.

		Providers			Single devices		Enterprises		Network of devices		Specific	
Issues	Characteristics	ISP	Cloud	Social networks	Mobile	Individuals	SMEs	Big enterprise	IoT	Sensor network	CSP	Industry
Evolution of systems	Dynamicity of system	H	H	H	H	M	M	M	H	M	L	L
	Evolution of technology	M	M	M	H	M	M	M	M	M	L	L
Information Asymmetry	Easy to change controls	H	H	H	H	H	M	H	M	M	L	L
	"Closed" security system	M	M	M	H	L	M	H	M	M	H	H
Hard to specify rate of occurrences	Evolution of threats	M	M	H	M	M	M	M	M	M	L	L
	Operational dependence	M	M	H	H	H	H	H	M	M	L	M
Lack of statistical data	Possibility to keep data hidden	M	M	L	H	M	M	M	L	M	M	H
	Scarcity of similar systems	M	M	L	L	L	M	M	M	M	H	H
Hard to estimate damage	Intangible impact	M	M	H	M	M	M	M	L	L	L	L
	Unpredictable impact	H	H	H	L	L	M	M	M	M	L	L
Interdependence of security	External interdependence of security	H	H	H	M	M	M	H	L	L	L	L
	Internal interdependence of security	H	H	H	L	L	M	H	M	M	H	H
Correlated risk	Geographical similarity	M	M	M	H	H	M	M	M	M	L	L
	Monoculture	M	M	H	H	H	M	M	M	M	L	L
	Simultaneous replication of attacks	M	M	M	H	H	H	M	M	M	L	L
Liability	Additional liability	H	H	H	L	L	M	H	M	M	H	H
Time to claim	Unnoticed attack	M	**M**	H	H	H	M	**M**	**M**	M	**L**	**L**

7.2.4. 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 law.

7.2.5. 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 approaches exist.

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 if the system is unique as a cyber–physical system or an industrial IT networks (see Table 8). One approach could be to re-use the information available for re-useable 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.

7.2.6. Interdependency of security

New theoretical approaches and practical studies. From the analysis of the literature in Section 6.2 we see that interdependent security has a negative impact on the incentive of insureds 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 [204]. Some domains in Table 8 have a specific topology. For example, internal structure of ISP can be seen as a star-shaped (sub-)network. Cloud services may be connected with some sort of a hierarchical topology model. Specific approaches for such topologies can help cyber risk predictions to become more precise.

7.2.7. Correlated risks

Evaluation of the real impact. There are many studies of interdependent security, but security incidents correlate not only because of weak security of others, 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 [82] 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 [127] 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 these domains either.

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.

7.2.8. 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. On the other hand, liability of providers may open new schemas for investment in cyber protection (e.g., as it is shown in [191] for a cyber insurer).

Simplify forensics burden. Many insurers require official forensics to be conducted before reimbursing the expenses. This is not always feasible for small incidents (like virus penetration) covered by insurance. Moreover, these incidents are not of primary importance for the LEAs. 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 incident notification, clue collection and analysis (e.g., with Big Data technologies) may promptly attract attention of LEAs to attacks cheap for individuals, but costly for a society.

8. Conclusion

In this paper we have 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 risks, as well as to contribute to societal welfare.

In this work we have considered the main topics tackled in the cyber insurance literature. Moreover, 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 although cyber insurance is a desirable option for agents it has many open issues yet to be resolved by scientists and practitioners. Novel approaches and treatments are required to ensure the positive effect of cyber insurance on society as well as new standards and practices required for the maturation of the market.

Our study also has provided analysis of different technological systems, which could be or are of interest for cyber insurers. We have found that different technological systems impose different challenges on cyber insurance, and, at the same time, provide different opportunities. Thus, more research is needed to address the needs of cyber insurance in specific contexts.

Finally, we have outlined a number of possible directions for solving the existing issues. Some of these directions are well-known in the 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 findings should be confirmed (e.g., correlated risks and interdependent security).

References

[1] World Economic Forum, Global risks 2014. ninth edition, available via http://www.droughtmanagement.info/literature/WEF_global_risks_report_2014.pdf on 03/01/2017 (2014).
[2] Department of Justice, Five indicted in new jersey for largest known data breach conspiracy, available via https://www.justice.gov/opa/pr/five-indicted-new-jersey-largest-known-data-breach-conspiracy 03/01/2017 (2013).
[3] D. Goodin, Meet great cannon, the man-in-the-middle weapon China used on github, available via http://arstechnica.com/security/2015/04/meet-great-cannon-the-man-in-the-middle-weapon-china-used-on-github/ on 03/01/2017 (2015).
[4] D. Murphy, Anonymous' 'operation blackout' goes dark; dns just fine, available via http://www.pcmag.com/article2/0,2817,2402469,00.asp on 03/01/2017 (2012).
[5] N. Gohring, Cyberinsurance may cover damage of computer woes, The Seattle Times, July 2002.
[6] Ponemon Institute LLC, Managing cyber security as a business risk: Cyber insurance in the digital age, available via https://www.experian.com/innovation/thought-leadership/ponemon-study-managing-cyber-security-as-business-risk.jsp?ecd_dbres_cyber_insurance_study_ponemon_referral on 03/01/2017 (August 2013).
[7] H.S.B. Herath, T.C. Herath, Cyber-insurance: Copula pricing framework and implication for risk management, in: WEIS, 2007.
[8] ENISA, Incentives and barriers of the cyber insurance market in Europe, available via http://goo.gl/BtNyj4 on 03/01/2017 (June 2012).
[9] M. Greisiger, Cyber liability & data breach insurance claims, available via https://netdiligence.com/wp-content/uploads/2016/05/CyberClaimsStudy-2013.pdf on 03/01/2017 (2013).
[10] R. Anderson, R. Böhme, R. Claytin, T. Moore, Security economics and the internal market, available via https://www.enisa.europa.eu/publications/archive/economics-sec/at_download/fullReport on 03/01/2017 (January 2008).
[11] L.A. Gordon, M.P. Loeb, T. Sohail, A framework for using insurance for cyber-risk management, Commun. ACM 46 (3) (2003) 81–85.
[12] T. Moore, The economics of cybersecurity: Principles and policy options, Int. J. Crit. Infrastruct. Prot. 3 (3–4) (2010) 103–117.
[13] D. Geer, Risk management is still where the money is, Computer 36 (12) (2003) 129–131.
[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, S. Shidore, Towards a managerial decision framework for utilization of cyber insurance instruments in it security, in: V. Sambamurthy, M. Tanniru (Eds.), AMCIS, Association for Information Systems, 2011.
[16] T. Poletti, First-ever insurance against hackers, available http://goo.gl/SSGArI on 03/01/2017 (June 1998).
[17] M.E. Kabay, ICSA White Paper Threats, Vulnerabilities and Real-World Responses: The Foundations of the TruSecure Process, ICSA, Inc. (1998).
[18] R.P. Majuca, W. Yurcik, J.P. Kesan, The evolution of cyberinsurance, Comput. Res. Repository (2006) 1–16.
[19] S. Mansfield-Devine, Security guarantees: building credibility for security vendors, Netw. Secur. 2016 (2) (2016) 14–18.
[20] EY, Global insurance outlook, available via http://goo.gl/uyFzQ4 on 03/01/2017 (2015).
[21] E.J. Vaughan, T.M. Vaughan, Fundamentals of Risk and Insurance, eleventh ed., Wiley, 2014.
[22] Advisen, Cyber insurance underwriting: A high-tech, evolving discipline, available via http://goo.gl/LxoQDq on 03/01/2017 (November 2014).
[23] 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 03/01/2017 (November 2012).
[24] R.S. Betterley, Cyber/privacy insurance market syurvey - 2015, available via http://betterley.com/samples/cpims15_nt.pdf on 03/01/2017 (June 2015).
[25] S. Jones, Lloyd's CEO Sees Cyber Insurance to Surge After Attacks, Bloomberg Business, available via http://goo.gl/kN58LV on 03/01/2017 (October 2014).
[26] C. Toregas, N. Zahn, Insurance for cyber attacks: The issue of setting premiums in context, Tech. Rep. GW-CSPRI-2014-1, The George Washington University, 2014, available via http://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/53c3daa5e4b056f825681c72/1405344421345/cyberinsurance_paper_pdf.pdf on 03/01/2017.

[27] 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 03/01/2017 (February 2014).
[28] F.B. Schneider, Enforceable security policies, ACM Trans. Inf. Syst. Secur. 3 (1) (2000) 30–50.
[29] W. Baer, Rewarding it security in the marketplace, Contemp. Secur. Policy 24 (1) (2003) 190–208.
[30] L. Clinton, D. Reddy, Can cyber insurance be linked to assurance?, 2015, available via https://www.rsaconference.com/writable/presentations/file_upload/cxo-w03-can-cyber-insurance-be-linked-to-assurance.pdf on 03/01/2017.
[31] R. Anderson, T. Moore, The economics of information security: A survey and open questions, Science 314 (2006) 610–613.
[32] R. Anderson, T. Moore, S. Nagaraja, A. Ozment, Incentives and Infrormation Security, Cambridge University Press, 2007, pp. 633–649 (Chapter 25).
[33] R. Böhme, Cyber-insurance revisited, in: Proceedings of the 4th Workshop on the Economics of Information Security, 2005.
[34] X. Zhao, L. Xue, 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, 2009, p. 49.
[35] H. Ogut, N. Menon, S. Raghunathan, Cyber insurance and it security investment: Impact of interdependent risk, in: Proceedings of the 4th Workshop on the Economics of Information Security, 2005.
[36] M. Lelarge, 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, Rio de Janeiro, Brazil, 2009, pp. 1494–1502.
[37] N. Shetty, G. Schwartz, J. Walrand, Can competitive insurers improve network security? in: A. Acquisti, S. Smith, A.-R. Sadeghi (Eds.), Proceedings of the 3rd International Conference on Trust and Trustworthy Computing, in: Lecture Notes in Computer Science, vol. 6101, Springer, Berlin, Heidelberg, 2010, pp. 308–322.
[38] G. Schwartz, N. Shetty, J. Walrand, Cyber-insurance: Missing market driven by user heterogeneity, in: WEIS, 2010.
[39] R. Pal, L. Golubchik, K. Psounis, P. Hui, Will cyber-insurance improve network security? A market analysis, in: Proceedings of the 2014 INFOCOM, IEEE, 2014, pp. 235–243.
[40] P. Naghizadeh, M. Liu, Voluntary participation in cyber-insurance markets, in: Proceedings of the 2014 Annual Workshop on Economics in Information Security, 2014.
[41] S. Radosavac, J. Kempf, U.C. Kozat, Using insurance to increase Internet security, in: J. Feigenbaum, Y.R. Yang (Eds.), NetEcon, ACM, 2008, pp. 43–48.
[42] R. Böhme, G. Schwartz, Modeling cyber-insurance: Towards a unifying framework, in: Proceedings of the 9th Workshop on the Economics in Information Security, 2010.
[43] B. Filkins, Quantifying risk: Closing the chasm between cybersecurity and cyber insurance, SANS Institute, available via https://www.sans.org/reading-room/whitepapers/leadership/quantifying-risk-closing-chasm-cybersecurity-cyber-insurance-36770 on 03/01/2017 (2016).
[44] A. Harrison, Counterpane offers Internet security insurance, COMPUTERWORLD, July 2000.
[45] C. Hemenway, Broker beat: Fierce competition for more cyber buyers, ADVISEN NEWS, available via http://www.advisenltd.com/insurance-news/2014/03/21/broker-beat-fierce-competition-cyber-buyers/ on 03/01/2017 (March 2014).
[46] C. State, Senate bill no. 1386 chapter 915, available http://goo.gl/W8qhb8 on 03/01/2017 (2002).
[47] Risk Management Solutions, Inc., Managing Cyber Insurance Accumulation Risk, available via on 03/01/2017 (2016).
[48] Australian Law Reform Commission, Data breach notification, available via http://goo.gl/ZZzanO on 01/03/2017.
[49] E. Parliament, European parliament legislative resolution of 12 March 2014 on general data protection regulation, October 2014.
[50] D. Heywood, Data breaches – what can we expect from the EU?, available via http://goo.gl/6Sa38Z on 03/01/2017 (January 2015).
[51] ACE group, ACE European risk briefing 2012. It and cyber risk, available via http://www.acegroup.com/global-assets/documents/Europe-Corporate/Risk-Briefing/European-Risk-Briefing\T1\ndash05.pdf on 03/01/2017.
[52] R.S. Betterley, Cyber/privacy insurance market survey - 2014, available via http://betterley.com/samples/cpims14_nt.pdf on 03/01/2017 (June 2014).
[53] Chubb, Cybersecurity for health care organizations, Available via http://www.chubb.com/businesses/csi/chubb15316.pdf on 03/01/2017.
[54] Advisen, 2016 survey of cyber insurance market trends, available via http://www.partnerre.com/assets/uploads/docs/PartnerRe_Cyber_Liability_Trends_Survey_2016.pdf on 03/01/2017 (October 2016).
[55] Allianz, Allianz cyber protect, available via http://www.agcs.allianz.com/services/financial-lines/allianz-cyber-protect/ on 13/07/2015.
[56] QBE European Operations, QBE Cyber and Data Security, available via http://goo.gl/zaZf9E on 17/03/2016.
[57] AEGIS, Cyber coverage & services, available via https://www.aegislink.com/aegislink/services/underwriting/products/cyber-coverage-and-services.html on 17/03/2016.
[58] CNA, Cyber liability, available via https://goo.gl/dtfTUU on 17/03/2016.
[59] InsureTrust, Cyber liability, available via http://www.insuretrust.com/cyber-liability/liability-package/cyber-liability on 17/03/2016.
[60] CDRM LLC, CDRM background and value proposition:, available via https://databreachinsurancequote.com/about-cyber-data-risk-managers/ 05/04/2016.
[61] Travelers, Lawyers professional liability coverage declarations, available via http://goo.gl/r2CXtB 17/03/2016.
[62] Zurich, Security and privacy, available via https://www.zurichna.com/en/industries/technology/secpriv on 17/03/2016.
[63] ACE, Privacy and network security, available via http://goo.gl/eq1Ll2 on 17/03/2016 (2015).
[64] Hiscox, E-risks insurance- summary of cover, avaliable via https://www.hiscox.co.uk/shared-documents/E-risks-insurance-summary-of-cover.pdf on 17/03/2016.
[65] Insureon, Cyber liability insurance, available via http://www.insureon.com/products/cyber-liability/ on 17/03/2016.
[66] Marsh, Cyber insurance, available via http://goo.gl/L2aFz5 on 17/03/2016 (2012).
[67] Chubb, Worth the risk? Finding from the chubb 2013 private company risk survey. (Chapter 7), available via http://www.chubb.com/businesses/csi/chubb12192.pdf on 17/03/2016 (2013).
[68] AIG, Cyberedge cyber liability insurance - policy wording, available via http://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-pc-policy-brochure.pdf on 17/03/2016.
[69] 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.
[70] 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 03/01/2017 (2010).
[71] J.P. Kesan, R.P. Majuca, W.J. Yurcik, The economic case for cybersinsurance, Tech. Rep. LE04-004, Illinois Law and Economics, 2004.
[72] C.J. Alberts, A.J. Dorofee, OCTAVE Criteria, Tech. Rep. CMU/SEI-2001-TR-016, CERT, 2001.
[73] D. Verdon, G. McGraw, Risk analysis in software design, IEEE Secur. Priv. 2 (4) (2004) 79–84.
[74] NIST, Guide for conducting risk assessment, Tech. Rep. SP 800-30 Revision 1, National Institute of Standards and Technology, 2012.
[75] R.A. Caralli, J.F. Stevens, L.R. Young, W.R. Wilson, Introducing octave allegro: Improving the information security risks assessment process, Tech. Rep. CMU/SEI-2007-TR-012, Software Engineering Institute, 2007.
[76] M.A. Amutio, J. Candau, MAGERIT- Methodology for Information Systems Risk Analysis and Management. Book I - The Method, third ed., Ministerio de HJacienda Y Administraciones Publicas, 2014.
[77] K. Kirkpatrick, Cyber policies on the rise, Commun. ACM 58 (10) (2015) 21–23.
[78] E. Chabrow, 10 concerns when buying cyber insurance, BankInfoSecurity, available via http://goo.gl/TT3Dqf on 03/01/2017 (June 2012).
[79] P.K. Rosen, B. Steinberg, M.K. Kearney, M.L. O'Connor, N.A. Rubin, Cyber insurance: A last line of defence when technology fails, avilavle via http://goo.gl/0NwDhO on 03/01/2017 (April 2014).
[80] I.A. Tondel, P.H. Meland, A. Omerovic, E.A. Gjaere, B. Solhaug, Using cyber-insurance as a risk management strategy: Knowledge gaps and recommendations for further research, available via https://goo.gl/wMesrj on 03/01/2017 (November 2015).
[81] R. Böhme, Security metrics and security investment models, in: I. Echizen, N. Kunihiro, R. Sasaki (Eds.), Proceedings of the 5th International Workshop on Security on Advances in Information and Computer Security, in: Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2010, pp. 10–24.
[82] C. Biener, M. Eling, 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 03/01/2017 (2014).
[83] A. Hedrick, Cyberinsurance: A risk management tool? in: Proceedings of the 4th Annual Conference on Information Security Curriculum Development, InfoSecCD'07, ACM, New York, NY, USA, 2007, pp. 20:1–20:4.
[84] L. Bailey, Mitigating moral hazard in cyber-risk insurance, JL Cyber Warfare 3 (1) (2014) 1–43.
[85] T. Bandyopadhyay, V.S. Mookerjee, R.C. Rao, A model to analyze the unfulfilled promise of cyber insurance: The impact of secondary loss, Working Paper, 2010.
[86] A. Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison-Wesley, 2007.
[87] L. Krautsevich, F. Martinelli, 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.
[88] W. Yurcik, 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.
[89] Armic, Airmic review of recent developments in the cyber insurance market, Tech. rep., Airmic Technical, 2012, Available via http://www.insurancehound.co.uk/abstract/airmic-review-recent-developments-cyber-insurance-market-13895 on 03/01/2017.

[90] PwC, Top issues. The promise and prifalls of cyber insurance, availavle via https://www.pwc.com/us/en/insurance/publications/assets/pwc-insurance-top-issues-cyber-insurance.pdf on 03/01/2017.
[91] M. Crane, International liability in cyberspace, Duke Law Technol. Rev. 1 (1) (2001) 23.
[92] W.S. Baer, A. Parkinson, Cyberinsurance in it security management, IEEE Secur. Priv. 5 (3) (2007) 50–56.
[93] PwC, Managing cyber risks with insurance, PricewaterhouseCoopers LLP, available via http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-managing-cyber-risks-with-insurance.pdf on 03/01/2017 (2014).
[94] S.J. Shackelford, Should your firm invest in cyber risk insurance? Bus. Horiz. 55 (4) (2012) 349–356.
[95] National Protection and Programs Directorate. Department of Homeland Security, Insurance industry working session readout report. Insurance for cyber-related critical infrastructure loss: Key issues, available via http://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf on 03/01/2017 (July 2014).
[96] P. Luzwick, If most of your revenue is from e-commerce, then cyber-insurance makes sense, Comput. Fraud Secur. 3 (2001) 16–17.
[97] 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, J. Westby, Data privacy, information security and cyber insurance trend, available via http://goo.gl/MnblUt on 03/01/2017 (2013).
[98] D.K. Saini, I. Azad, N.B. Raut, L.A. Hadimani, Utility implementation for cyber risk insurance modeling, in: Proceedings of the World Congress on Engineering, Vol. 1, 2011.
[99] A.R. Willis, Business insurance: First-party commercial property insurance and the physical damage requirement in a computer-dominated world, Florida State Univ. Law Rev. 37 (4) (2010) 1–22.
[100] P.H. Meland, I.A. Tondel, B. Solhaug, Mitigating risk with cyberinsurance, IEEE Secur. Privacy 13 (6) (2015) 38–43.
[101] T. Bandyopadhyay, V.S. Mookerjee, R.C. Rao, Why it managers don't go for cyber-insurance products, Commun. ACM 52 (11) (2009) 68–73.
[102] G. Schwartz, N. Shetty, J.C. Walrand, Why cyber-insurance contracts fail to reflect cyber-risks, in: Proceeding Sof the 51st Annual Allerton Conference, 2013, pp. 781–787.
[103] G.A. Schwartz, 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, ACM, New York, NY, USA, 2014, pp. 14–154.
[104] M. Lelarge, J. Bolot, Network externalities and the deployment of security features and protocols in the Internet, SIGMETRICS Perform. Eval. Rev. 36 (1) (2008) 37–48.
[105] R. Mehr, E. Cammack, Principles of Insurance, third ed., Richard D. Irwin, Inc., 1961.
[106] B. Berliner, Large risks and limits of insurability, Geneva Pap. Risk Insur. 10 (37) (1985) 313–329.
[107] C. Biener, M. Eling, J.H. Wirfs, Insurability of cyber risk, Newslett. Insur. Financ. (14) (2014) 1–4.
[108] J. von Neumann, O. Morgenstern, Theory of Games and Economic Behaviour, third ed., Princeston University Press, 1953.
[109] W. Rudin, Real and Complex Analysis, third ed., McGraw-Hill, 1987.
[110] Z. Yang, J.C.S. Lui, Security adoption and influence of cyber-insurance markets in heterogeneous networks, Perform. Eval. 74 (2014) 1–17.
[111] American Insurance Association, Property-casualty insurance basics, available via http://goo.gl/M06lRg on 03/01/2017.
[112] T. Mikosch, Non-Life Insurance Mathematics, Springer, 2009.
[113] C. Barracchini, M.E. Addessi, Cyber risk and insurance coverage: An actuarial multistate approach, Rev. Econ. Finanac. 4 (2014) 57–69.
[114] S. Chaisiri, R.K.L. Ko, D. Niyato, A joint optimization approach to security-as-a-service allocation and cyber insurance management, in: Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Vol. 1, 2015, pp. 426–433.
[115] A.N. Yannacopoulos, C. Lambrinoudakis, S. Gritzalis, S.Z. Xanthopoulos, S.N. Katsikas, Modeling privacy insurance contracts and their utilization in risk management for ict firms, in: S. Jajodia, J. Lopez (Eds.), Proceedings of 13th European Symposium on Research in Computer Security, Vol. 5283, Springer, Berlin, Heidelberg, 2008, pp. 207–222.
[116] A. Hofmann, Internalizing externalities of loss prevention through insurance monopoly: an analysis of interdependent risks, Geneva Risk Insur. Rev. 32 (2007) 91–111.
[117] R. Pal, L. Golubchik, On economics of information security: The problem of designing optimal cyber-insurance contracts, in: Proceedings of ACM SIGMETRICS Workshop, 2010.
[118] R. Pal, L. Golubchik, K. Psounis, Aegis a novel cyber-insurance model, in: J. Baras, J. Katz, E. Altman (Eds.), Decision and Game Theory for Security, in: Lecture Notes in Computer Science, vol. 7037, Springer, Berlin, Heidelberg, 2011, pp. 131–150.
[119] J. Bolot, M. Lelarge, A new perspective on Internet security security using insurance, Tech. Rep. RR-6329, INRIA, 2007.
[120] J. Bolot, M. Lelarge, A new perspective on Internet security using insurance, in: Proceedings of the 27th IEEE International Conference on Computer Communications, Phoenix, AZ, USA, 2008, pp. 1948–1956.
[121] N. Shetty, G. Schwartz, M. Felegyhazi, J. Walrand, Competitive cyber-insurance and internet security, in: Economics of Information Security and Privacy, Springer, US, 2010, pp. 229–247.
[122] J. Grossklags, N. Christin, J. Chuang, Secure or insure?: A game-theoretic analysis of information security games, in: Proceedings of the 17th International Conference on World Wide Web, WWW'08, ACM, New York, NY, USA, 2008, pp. 209–218.
[123] J. Grossklags, B. Johnson, Uncertainty in the weakest-link security game, in: Proceedings of the 1st International Conference on Game Theory for Networks, 2009.
[124] B. Johnson, J. Grossklags, N. Christin, J. Chuang, Nash equilibria for weakest target security games with heterogeneous agents, in: R. Jain, R. Kannan (Eds.), Proceedings of the 2nd International ICST Conference on Game Theory for Networks, in: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, Berlin, Heidelberg, 2012, pp. 444–458.
[125] R. Böhme, G. Kataria, Models and measures for correlation in cyber-insurance, in: Proceedings of the 5-th Workshop on Economics of Information Security, 2006.
[126] X. Zhao, L. Xue, A.B. Whinston, 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, 2009, p. 49.
[127] W. Shim, An analysis of information security management strategies in the presence of interdependent security risk, Asia Pac. J. Inf. Syst. 22 (1) (2012) 79–101.
[128] S. Gritzalis, A.N. Yannacopoulos, C. Lambrinoudakis, P. Hatzopoulos, S.K. Katsikas, A probabilistic model for optimal insurance contracts against security risks and privacy violation in it outsourcing environments, Int. J. Inf. Secur. 6 (4) (2007) 197–211.
[129] C. Lambrinoudakis, S. Gritzalis, P. Hatzopoulos, A.N. Yannacopoulos, S. Katsikas, A formal model for pricing information systems insurance contracts, Comput. Stand. Interfaces 27 (5) (2005) 521–532. Formal Methods, Techniques and Tools for Secure and Reliable Applications.
[130] A. Shah, S. Dahake, S.H. Haran, Valuing data security and privacy using cyber insurance, SIGCAS Comput. Soc. 4 (1) (2015) 38–41.
[131] B. Johnson, R. Böhme, J. Grossklags, Security games with market insurance, in: J.S. Baras, J. Katz, E. Altman (Eds.), Proceedings of the Second International Conference on Decision and Game Theory for Security, in: Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2011, pp. 117–130.
[132] R. Pal, L. Golubchik, On the economics of information security: The problem of designing optimal cyber-insurance contracts, SIGMETRICS Perform. Eval. Rev. 38 (2) (2010) 51–53.
[133] R. Pal, L. Golubchik, Pricing and investments in Internet security: A cyber-insurance perspective, CoRR abs/1103.1552, 2011, pp. 1–30.
[134] R. Pal, L. Golubchik, K. Psounis, P. Hui, Realizing efficient cyber-insurance markets via price discriminating security products, available via http://www-scf.usc.edu/~rpal/TDSCR.pdf (2013).
[135] R. Pal, L. Golubchik, K. Psounis, 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, Brooklyn, New York, USA, 2013, pp. 1–9.
[136] R. Pal, P. Hui, On differentiating cyber-insurance contracts a topological perspective, in: Proceedings of the 2013 IFIP/IEEE International Symposium on Integrated Network Management, 2013, pp. 836–839.
[137] R. Pal, P. Hui, Cyberinsurance for cybersecurity a topological take on modulating insurance premiums, SIGMETRICS Perform. Eval. Rev. 40 (3) (2012) 86–88.
[138] S. Shavell, On moral hazard and insurance, in: Foundations of Insurance Economics, in: Readings in Economics and Finance, Springer, 1992, pp. 280–302.
[139] A. Laszka, M. Felegyhazi, L. Buttyan, A survey of interdependent information security games, ACM Comput. Surv. 47 (2) (2014) 23:1–23:38.
[140] J. Grossklags, S. Radosavac, A.A. Cárdenas, J. Chuang, Nudge: Intermediaries' role in interdependent network security, in: A. Acquisti, S.W. Smith, A.-R. Sadeghi (Eds.), Proceedings of the 3rd International Conference on Trust and Trustworthy Computing, in: Lecture Notes in Computer Science, vol. 6101, Springer, Berlin, Heidelberg, 2010, pp. 323–336.
[141] Microsoft, The security risk management guide, available via https://technet.microsoft.com/en-us/library/cc163143.aspx on 03/01/2017 (2006).
[142] CLUSIF, Risk Management - Concepts and Methods, Club de la securite de l'infromation francias, 30, rue Pierre Semard, 75009, Paris (2009).
[143] G. Stoneburner, A. Goguen, A. Feringa, Risk management guide for information technology systems, Tech. Rep. 800-30, National Institute of Standards and Technology, 2001, Available via http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf on 03/01/2017.
[144] ISO/IEC, ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements (2013).
[145] IEC, BS IEC 61882:2001. Hazard and operability studies (HAZOP studies) – Application guide (2001).
[146] A. Bouti, D.A. Kadi, A state-of-the-art review of FMEA/FMECA, Int. J. Reliab. Qual. Saf. Eng. 1 (4) (1994) 515–543.
[147] CLUSIF, Mehari 2010. Overview, Club De La Securite De L;Information Francias (2010).
[148] CLUSIF, Mehari 2010. Risk analysis and tratment guide, Club De La Securite De L'Information Francias (August 2010).
[149] CLUSIF, Mehari 2010. Processing guide for risk analysis and management, Club De La Securite De L'Information Francias, 2nd Edition (April 2011).
[150] ISO/IEC, ISO/IEC 27002:2005 Information technology – Security techniques – Code of Practice for Information Security Management (2005).

[151] M.S. Lund, B. Solhaug, K. Stølen, Model-Driven Risk Analysis, Springer, 2011.
[152] R. Fredriksen, M. Kristiansen, B.A. Gran, K. Stølen, T.A. Opperud, 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, in: Lecture Notes in Computer Science, vol. 2434, 2002, pp. 94–105.
[153] K. Stolen, F.D. Braber, T. Dimitrakos, R. Fredriksen, B.A. Gran, S.-H. Houmb, S. Lund, Y.C. Stamatiou, J.O. Aagedal, Model-based risk assessment – the CORAS approach, in: Proceedings of the 1st iTrust Workshop, 2002.
[154] B.A. Gran, R. Fredriksen, A.P.-J. Thunem, An approach for model-based risk assessment, in: SAFECOMP, 2004, pp. 311–324.
[155] F. Braber, I. Hogganvik, M.S. Lund, K. Stolen, F. Vraalsen, Model-based security analysis in seven steps – a guided tour to the coras method, BT Technol. J. 2 (1) (2007) 101–117.
[156] S.A. Butler, Security attribute evaluation method: a cost-benefit approach, in: Proceedings of the 24th International Conference on Software Engineering, (ICSE'02), ACM Press, 2002, pp. 232–240.
[157] B. Karabacak, I. Sogukpinar, Isram: information security risk analysis method, Comput. Secur. 24 (2) (2005) 147–159.
[158] S.P. Bennett, 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, IEEE Computer Society Press, 1992, pp. 64–73.
[159] F. Farahmand, S.B. Navathe, P.H. Enslow, G.P. Sharp, Managing vulnerabilities of information systems to security incidents, in: ICEC '03: Proceedings of the 5th International Conference on Electronic Commerce, ACM, New York, NY, USA, 2003, pp. 348–354.
[160] C.-C. Hsu, B.A. Sandford, The delphi technique: Making sense of consensus, Pract. Assess. Res. Eval. 12 (10) (2007) 1–8.
[161] J.H. Pardue, P. Patidar, Threats to healthcare data: a threat tree for risk assessment, Issues Inf. Syst. XII (1) (2011) 106–113.
[162] IEC, IEC 61025:2006. Fault tree analysis (FTA) (2006).
[163] B. Schneier, Attack trees: Modelling security threats, Dr. Dobb's J. (1999).
[164] S. Mauw, M. Oostdijk, Foundations of attack trees, in: Proceedings of the 8th International Conference on Information Security and Cryptology, in: Lecture Notes in Computer Science, Springer-Verlag, 2005.
[165] S. Bistarelli, M. Dall'Aglio, P. Peretti, Strategic games on defense trees, in: Proceedings of 4th International Workshop on Formal Aspects in Security and Trust, 2007, pp. 1–15.
[166] R. von Solms, J.V. Niekerk, From information security to cyber security, Comput. Secur. 38 (2013) 97–102.
[167] ISACA, Cobit 5, Avalaible via http://www.isaca.org/COBIT/Pages/default.aspx on 03/01/2017.
[168] IASME Consortium, The IASME Standard, Available via https://www.iasme.co.uk/index.php/about on 03/01/2017.
[169] 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 03/01/2017.
[170] NERC, Cip-002-4 – cyber security – critical cyber asset identification, available via http://goo.gl/5i6zxg on 03/01/2017.
[171] NEN, Nen 7510:2011 nl - health informatics - information security management in healthcare, available via https://goo.gl/5pk0oT on 03/01/2017.
[172] 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 03/01/2017.
[173] C. Morrison, AIG offers SME protection against "hacktivists" with new cyber product, available via www.insuranceage.co.uk/insurance-age/news/2367528/aig-offers-sme-protection-against-hacktivists-with-new-cyber-product on 03/01/2017 (September 2014).
[174] IEC, IEC 60300-3-9 Dependability management- Part 3. Application guide - Section 9: Risk analysis of technological systems - Event Tree Analysis (ETA) (1995).
[175] R. Ortalo, Y. Deswarte, M. Kaaniche, Experimenting with quantitative evaluation tools for monitoring operational security, IEEE Trans. Softw. Eng. 25 (5) (1999) 633–650.
[176] O. Sheyner, J. Wing, Tools for generating and analysing attack graphs, in: Proceedings of Formal Methods for Components and Objects, in: Lecture Notes in Computer Science, Springer-Verlag, 2005.
[177] S. Noel, 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, ACM Press, New York, NY, USA, 2004, pp. 109–118.
[178] C. Phillips, L.P. Swiler, A graph-based system for network-vulnerability analysis, in: Proceedings of the 1998 Workshop on New Security Paradigms, ACM Press, 1998, pp. 71–79.
[179] L. Krautsevich, F. Martinelli, A. Yautsiukhin, Towards modelling adaptive attacker's behaviour, in: In Proceedings of 5th International Symposium on Foundations & Practice of Security, in: Lecture Notes on Computer Science, vol. 7743, Springer-Verlag, 2012, pp. 357–364.
[180] K. Beckers, L. Krautsevich, A. Yautsiukhin, Analysis of social engineering threats with attack graphs, in: Proceedings of the 3rd International Workshop on Quantitative Aspects in Security Assurance, in: Lecture Notes in Computer Science, Springer-Verlag, 2014.
[181] Snort, Snort, available via https://www.snort.org/ on 03/01/2017.
[182] L.A. Gordon, M.P. Loeb, Managing Cybersecurity Resources: a Cost-Benefit Analysis, McGraw Hill, 2006.
[183] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, S.K. Sadhukhan, Cyber-risk decision models: To insure it or not? Decis. Support Syst. 56 (2013) 11–26.
[184] A. Mukhopadhyay, G.K. Shukla, P. Kirs, 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.
[185] T. Ishikawa, K. Sakurai, A study of security management with cyber insurance, in: Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication, ACM, 2016, p. 68.
[186] Y. Hayel, Q. Zhu, Attack-aware cyber insurance for risk sharing in computer networks, in: M. Khouzani, E. Panaousis, G. Theodorakopoulos (Eds.), Proceedings of the 6th International Conference on Decision and Game Theory for Security, in: Lecture Notes in Computer Science, Springer International Publishing, Cham, 2015, pp. 22–34.
[187] J. Bolot, M. Lelarge, Cyber insurance as an incentive for internet security, in: Managing Information Risk and the Economics of Security, Springer, US, 2009, pp. 269–290.
[188] B. Johnson, A. Laszka, J. Grossklags, How many down?: toward understanding systematic risk in networks, in: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, ACM, 2014, pp. 49–500.
[189] A. Laszka, B. Johnson, J. Grossklags, M. Felegyhazi, Estimating systematic risk in real-world networks, in: Financial Cryptography and Data Security, Springer, 2014, pp. 417–435.
[190] B. Johnson, A. Laszka, J. Grossklags, The complexity of estimating systematic risk in networks, in: Proceedings of the 27th IEEE Computer Security Foundations Symposium, CSF, 2014.
[191] A. Laszka, J. Grossklags, Should cyber-insurance providers invest in software security? in: Computer Security–ESORICS 201, Springer, 2015, pp. 483–502.
[192] R. Pal, P. Hui, The impact of secure oss on Internet security: What cyber-insurers need to know, Tech. Rep, 2012, arXiv:1202.088, CoRR, available via https://arxiv.org/abs/1202.0885 on 03/01/2017.
[193] F. Martinelli, A. Yautsiukhin, Security by insurance for services, in: Proceedings of the 1st International Workshop on Cyber Resilience Economics, 2016.
[194] J. Grossklags, N. Christin, J. Chuang, Security and insurance management in networks with heterogeneous agents, in: Proceedings of the 9th ACM Conference on Electronic Commerce, EC'08, ACM, New York, NY, USA, 2008, pp. 160–169.
[195] B. Johnson, J. Grossklags, N. Christin, J. Chuang, Are security experts useful? Bayesian nash equilibria for network security games with limited information, in: D. Gritzalis, B. Preneel, M. Theoharidou (Eds.), Proceedings of the 15th European Symposium on Research in Computer Security, Springer, Berlin, Heidelberg, 2010, pp. 588–606.
[196] J. Grossklags, B. Johnson, N. Christin, Financial cryptography and data security: 14th international conference, fc 2010, tenerife, canary islands, january 25-28, 2010, revised selected papers, in: R. Sion (Ed.), Proceedings of the 14th International Conference on Financial Cryptography and Data Security, in: Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2010, pp. 416–423. Ch. When Information Improves Information Security.
[197] J. Grossklags, B. Johnson, N. Christin, The price of uncertainty in security games, in: Economics of Information Security and Privacy, Springer, 2010, pp. 9–32.
[198] I. Ehrlich, G.S. Becker, Market Insurance, Self-Insurance, and Self-Protection, Springer, Netherlands, Dordrecht, 1992, pp. 164–189.
[199] R. Pal, Cyber-insurance for cyber-security: a solution to the information asymmetry problem, in: Proceedings of SIAM Annual Meeting, 2012.
[200] R. Pal, Cyber-insurance in Internet security: A dig into the information asymmetry problem, Comput. Res. Repository (2012) 1–6.
[201] D.S. Herrmann, Complete Guide to Security and Privacy Metrics. Measuring Regulatory Compliance, Operational Resilience, and ROI, Auerbach Publications, 2007.
[202] L. Krautsevich, F. Martinelli, A. Yautsiukhin, Formal analysis of security metrics and risk, in: Proceedings of the IFIP Workshop on Information Security Theory and Practice, in: Lecture Notes in Computer Science, vol. 6633, Springer-Verlag, 2011, pp. 304–319.
[203] L. Krautsevich, F. Martinelli, A. Yautsiukhin, Formal analysis of security metrics with defensive actions, in: The 10th IEEE International Conference on Autonomic and Trusted Computing, IEEE, 2013.
[204] PwC, Managing cyber risks in an interconnected world, available via http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf on 03/01/2017 (September 2014).

Angelica Marotta is a research assistant within the security group at the IIT-CNR in Pisa. She received her Bachelor's Degree in Computer Science from the University of Pisa, Italy and she is currently pursuing graduate studies in cyber security at Southern New Hampshire University, NH, USA where she is gaining a global understanding of how to deal with cyber security threats from a scientific, legal, and organisational perspective. Her main areas of research cover risk management, cyber security and cyber insurance.

Fabio Martinelli received the M.Sc. degree from the University of Pisa, Pisa, Italy, in 1994 and the Ph.D. degree from the University of Siena, Siena, Italy, in 1999. He is currently a Senior Researcher with the Institute of Informatics and Telematics of the Consiglio Nazionale delle Ricerche, Pisa, Italy, where he leads the Cyber Security Project. He has co-authored more than 200 papers in international journals and conference or workshop proceedings. He is involved in several steering committees of international WGs or conferences and workshops. He manages research and development projects on information and communication security. His main research interests include security and privacy in distributed and mobile systems and foundations of security and trust.

Stefano Nanni received the master of Engineering degree from the University of Pisa, Pisa, Italy, in 1999 and the master in Insurance and Risk Management degree from the MIB School of Management, Trieste, Italy, in 2006. He is a Certified Financial Risk Manager and, after an early career in system integration, he ran various Risk and Control projects at PwC and then at Zurich Insurance Group. He is currently responsible for open innovation at Unipol Gruppo Finanziario S.p.A. He is a contributor to the Network and Information Security Public–Private Platform of the European Union and leads the Big Data initiative of the Chief Risk Officers Forum, an interest group whose members are large multinational insurance companies.

Albina Orlando received the M.Sc. degree in Economics in 1996 and the Ph.D. degree in Financial Mathematics and Actuarial Science in 2000 from the University of Napoli "Federico II", Napoli Italy. She is currently a Researcher with IAC "Mauro Picone" of the Consiglio Nazionale delle Ricerche, Napoli, Italy. From 2005 to 2009 she was Adjunct Professor in Mathematics for Economics at the University of Salerno. She is currently Adjunct Professor in Advanced Financial Mathematics at the University of Napoli "Federico II" and teaches Financial Mathematics at the Master program of the Scuola di Alta formazione IPE, Napoli, Italy. Her research interests lie in Mathematical models for insurance sciences, Risk management in life insurance and Stochastic mortality models.

Artsiom Yautsiukhin received the M.Sc. degree from Belorussian State University, Minsk, Belarus, in 2004 and the Ph.D. degree in information and communication technology, University of Trento, Trento, Italy, in 2009. He is a Researcher with the Information Security Group, Institute of Informatics and Telematics of the Consiglio Nazionale delle Ricerche, Pisa, Italy. He has co-authored of more than 30 papers in the international journals, workshops and conferences and also participated in a number of European projects. His research interests include, but are not limited to, assessment of security, security metrics and risk, security assessment of complex business systems, and risk-based usage control.

Please cite this article in press as: A. Marotta, et al., Cyber-insurance survey, Computer Science Review (2017), http://dx.doi.org/10.1016/j.cosrev.2017.01.001