THE GENEVA ASSOCIATION

Ten Key Questions on Cyber Risk and Cyber Risk Insurance

THE GENEVA ASSOCIATION

November 2016

The Geneva Association

The Geneva Association is the leading international insurance think tank for strategically important insurance and risk management issues. The Geneva Association identifies fundamental trends and strategic issues where insurance plays a substantial role or which influence the insurance sector. Through the development of research programmes, regular publications and the organisation of international meetings, The Geneva Association serves as a catalyst for progress in the understanding of risk and insurance matters and acts as an information creator and disseminator. It is the leading voice of the largest insurance groups worldwide in the dialogue with international institutions. In parallel, it advances—in economic and cultural terms—the development and application of risk management and the understanding of uncertainty in the modern economy.

The Geneva Association membership comprises a statutory maximum of 90 chief executive of officers (CEOs) from the world's top insurance and reinsurance companies. It organises international expert networks and manages discussion platforms for senior insurance executives and specialists as well as policymakers, regulators and multilateral organisations.

Established in 1973, The Geneva Association, officially the 'International Association for the Study of Insurance Economics', is based in Zurich, Switzerland and is a non-profit organisation funded by its Members.

Ten Key Questions on Cyber Risk and Cyber Risk Insurance

by Martin Eling, Werner Schnell, edited by Fabian Sommerrock

Martin Eling, Werner Schnell—Institute of Insurance Economics, University of St. Gallen

Fabian Sommerrock—Deputy Secretary General and Head of Insight, The Geneva Association

The Geneva Association

The Geneva Association—'International Association for the Study of Insurance Economics'
Zurich | Talstrasse 70, CH-8001 Zurich
Email: secretariat@genevaassociation.org | Tel: +41 44 200 49 00 | Fax: +41 44 200 49 99

Photo Credits:
Cover page— Garik Barseghyan, Shutterstock.

November 2016

Ten Key Questions on Cyber Risk and Cyber Risk Insurance.

Published by The Geneva Association—'International Association for the Study of Insurance Economics', Zurich.

Download the electronic version from *www.genevaassociation.org*.

Contents

Acknowledgements

This paper was prepared as part of The Geneva Association research programme 'Cyber & Innovation' and greatly profited from discussions with numerous academics and practitioners. We are especially grateful to Daljitt Barn (Munich Re), Nick Beecroft, Trevor Maynard (Lloyd's), Maya Bundt, Eric Durand (Swiss Re), José Fidalgo (Allianz), David Ho, Tracie Grella (AIG), Benno Keller (Zurich), Philipp Lienau, Patrick Smolka (HDI Global), Susan Penwarden, Mark Dunham (Aviva UK), Erwin Groeneveld (Aegon), and Jan Wirfs (IVW, University of St. Gallen) for valuable feedback and comments.

Foreword

Anna Maria D'Hulster

Secretary General,
The Geneva Association

Information and communications technology (ICT) has become an essential contributor to our daily lives. Not only is it the engine of trade and of the global financial system, but it is also a vital component of our most critical infrastructure. In simple terms, the networks that provide our water, food, electricity, communications and transportation are all dependent on ICT.

The advent of user-generated content on the Internet, so-called Web 2.0, is also creating vast pools of (individual) specific data, some of which are highly sensitive, not least because they comprise financial, behavioural, health and other personal information. These data are a rich source of insights on individual and collective attitudes and behaviours and can be of tremendous value to both commercial and public institutions who are now harvesting and storing this data.

With our reliance on ICT and the value of this data come risks to its security, integrity and failure. This cyber risk can either have a natural cause or be man-made, where the latter can emerge from human failure, cyber criminality (e.g. extortion, fraud), cyberwar, and cyber terrorism. Currently, cyber risk is still in its infancy, but it has the power to constrain the forward momentum of technology and adversely impact the world economy.

The development of a cyber insurance market is still at an early stage. While protection against cyber risk represents a tremendous new market and an opportunity for the insurance industry, it also creates a number of challenges to insurability. These include its potential high complexity and interdependencies, the potential extreme events it can cause, high uncertainty with respect to data availability and modelling approach, and ongoing technological change. However, anecdotally it is not only the challenge of insurability but also the demand for products that is hampering the market's development. Either way, the successful development of a cyber risk insurance market is an important goal for the further development of society.

In 2016, The Geneva Association established a new research programme on Cyber and Innovation. The programme provides inter alia a platform for industry discussion on cyber risk and insurance and will seek to develop and inspire research and insights that support its development. This report is the first of the programme and is intended as a 'primer' on cyber risk and cyber risk insurance for different stakeholders (academia, the insurance industry, governments and policymakers as well as the wider public). By providing an overview of the main areas of research and the key studies conducted in the field to date, and by making some initial recommendations about the potential role of insurers and governments in addressing cyber risks, this report lays the groundwork for discussion and future research on the development of the cyber risk and the cyber insurance market.

1. Motivation and Aim of the Paper

In spite of its increasing relevance for businesses today, research on cyber risk is limited.[1] Many papers have been devoted to the technological aspects, but relatively little research has been published in the business and economics literature. The existing articles emphasise the lack of data and the modelling challenges (e.g. Maillart and Sornette 2010; Biener, Eling and Wirfs, 2015), the complexity and dependent risk structure (e.g. Hofmann and Ramaj, 2011; Ögüt, Raghunathan, and Menon, 2011) or adverse selection and moral hazard issues (e.g. Gordon, Loeb, and Sohail, 2003). More recent research is concerned with potentially huge losses from worst-case scenarios such as the breakdown of critical information infrastructure (e.g. World Economic Forum, 2010; Ruffle *et al*., 2014; Lloyd's, 2015b; Long Finance, 2015). In short, existing studies highlight challenges in the risk management and insurability of cyber risks.

The aim of this paper is to establish a database on studies, articles and working papers on cyber risk and cyber risk insurance.[2] Based on this, we provide insurance practitioners and academics a high-level overview of the main research topics and future research directions in the field. The focus of the analysis will be on the business and economics literature in the risk and insurance domain. In order to provide a structured discussion of the relevant literature, we structure our analysis around three research clusters and 10 key questions (***see Figure 1***).

The paper begins by summarising the existing knowledge on cyber risk and cyber insurance. Here we provide a structured review of the existing literature considering seven main research questions, starting with the definition of cyber risk followed by a review of the cyber insurance market. Based on these results we then derive future work both from an academic and from a practical perspective; that is, we consider what the industry and the government[3] could do in order to manage, insure, and prevent cyber risk. Moreover, potential research questions for academics are formulated.

1 As shown in Appendix A, research on the topic of cyber risk and cyber insurance has been very limited until the year 2010, but recently has been growing exponentially. This emphasises the increasing relevance of the topic both from a practical and academic perspective.

2 In this paper, we use the terms 'cyber risk insurance' and 'cyber insurance' interchangeably.

3 Our view on the government includes all potential activities by public authorities including legislation, regulation, and other work by the authorities.

Figure 1: Research approach with three clusters and ten key questions

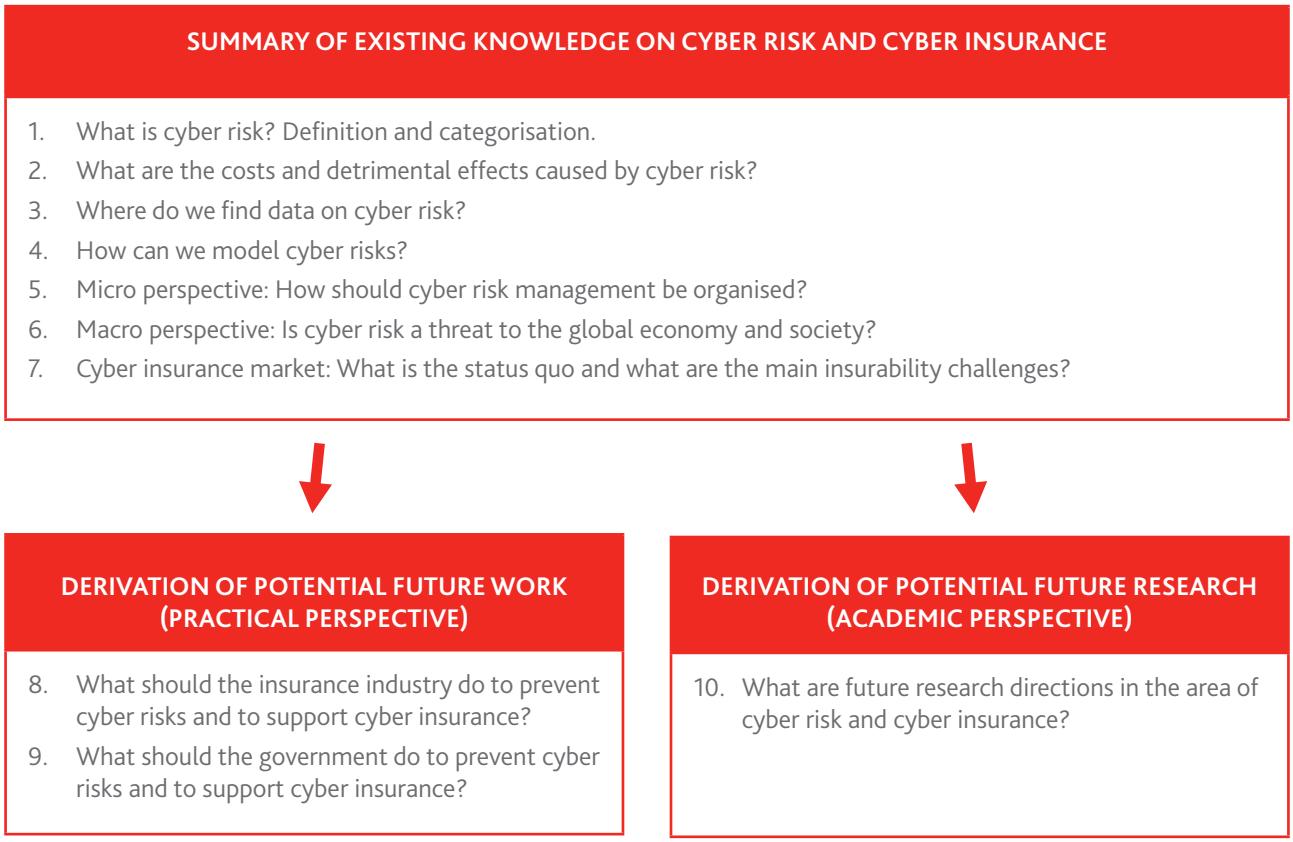


Table 1 (overleaf) lists the main results for the 10 research questions. The review outcomes for questions 1 to 7 illustrate the immense insurability challenges, especially due to the lack of data and of a modelling approach, the risk of change and an incalculable accumulation risk. Based upon these results, various ways to overcome these limitations in insurability are discussed such as mandatory reporting requirements, pooling of data, or public–private partnerships with the government (see the answers to questions 8 to 10).

The remainder of this paper is structured as follows. First, we briefly outline the research approach and present descriptive statistics on the review results (Section 2). Then in Section 3, we summarise the existing knowledge on cyber risk along the seven outlined key questions. Finally, we derive avenues for future work both from an industry and government (Section 4) and from an academic perspective (Section 5).

Table 1: Summary of results

1 What is cyber risk? Definition and categorisation.

- Any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology (OT) eventually leads to business disruption, (critical) infrastructure breakdown, and physical damage to humans and property.
- Cyber risk is either caused naturally or is man-made, where the latter can emerge from human failure, cyber criminality (e.g. extortion, fraud), cyberwar, and cyber terrorism. It is characterised by interdependencies, potential extreme events, high uncertainty with respect to data and modelling approach, and risk of change.

2 What are the costs and detrimental effects caused by cyber risk?

- The enormous global costs estimates (up to one trillion USD per year) published by software firms and consultants are rough estimators that need to be critically questioned.
- The manifold detrimental effects have been analysed, e.g. using event studies and scenario analyses. The major part of the effects are indirect (reputation, loss of trust).

3 Where do we find data on cyber risk?

- Data on cyber risk are scarce, e.g. because the victims are reluctant to report such events.
- Most empirical papers on cyber risk rely on data breach information (not loss information), but recently, first loss databases have been set up (NetDiligence (2014) in the U.S.; Biener *et al.* (2015) globally).

4 How can we model cyber risks?

- Frequency and severity modelling of cyber risk can be done by applying extreme value theory and the peaks over threshold approach. Heavy tail distributions have been proposed, i.e. the power law or the log-normal distribution for the severity and negative binomial distribution for the frequency.
- The aggregation of cyber risk needs to take nonlinear dependence into account (typically applying copulas). The few existing modelling papers emphasise the immense modelling difficulties and risk of change. Scenario analysis is a popular tool in such situations.

5 Micro perspective: How should cyber risk management be organised?

- There are special standards and tools for cyber risk management. In each step of the classical risk management process, cyber risks show special features.
- Institutional commitment, effective crisis management, risk communication with employees, customers and suppliers, and continuous monitoring are fundamental. Cyber risk management today focuses on risk mitigation, while risk transfer so far plays only a minor role.

6 Macro perspective: Is cyber risk a threat to the global economy and society?

- A global failure of the Internet is rather unlikely, but regionally limited breakdowns have already occurred; given the globally connected economy and society, the potential consequences of such extreme scenarios on companies and individuals are massive.
- The same holds for other cyber scenarios such as, for example, the blackout of energy systems. For insurers, such scenarios pose enormous accumulation risk and hamper insurability.

7 Cyber insurance market: What is the status quo and what are the main insurability challenges?

- The cyber insurance market is very small at present compared to other lines of business, but is expected to increase significantly in the coming years. The U.S. is far ahead of Europe and Asia, for example, with regard to reporting requirements.
- The main insurability problems are the lack of data, risk of change, accumulation risk, and potential moral hazard problems.

8 What should the insurance industry do to prevent cyber risks and to support cyber insurance?

- To prevent cyber risks: develop standards, common language, and good practices; conduct scenario analysis; initiate and/or intensify dialogue with stakeholders; track technological development (cloud computing, Internet of Things, blockchain technology etc.), increase own analytical skills (digital forensic) and make own IT more resilient.
- To support cyber insurance: develop anonymised data pools, develop (re-)insurance pools, analyse existing policies and develop new ones.

9 What should the government do to prevent cyber risks and to support cyber insurance?

- To prevent cyber risks: tackle cybercrime by international collaboration, initiate global dialogues and conventions aimed at confining cyberwars, boost IT landscape resilience, introduce reporting requirements, support development of cyber databases, and minimum standards for risk mitigation.
- To support cyber insurance: establish public–private partnership with government as insurer of last resort (governmental backstop for extreme scenarios); incentivise the development of an anonymised data pool; incentivise the development of traditional and alternative risk transfer mechanisms.

10 What are future research directions in the area of cyber risk and cyber insurance?

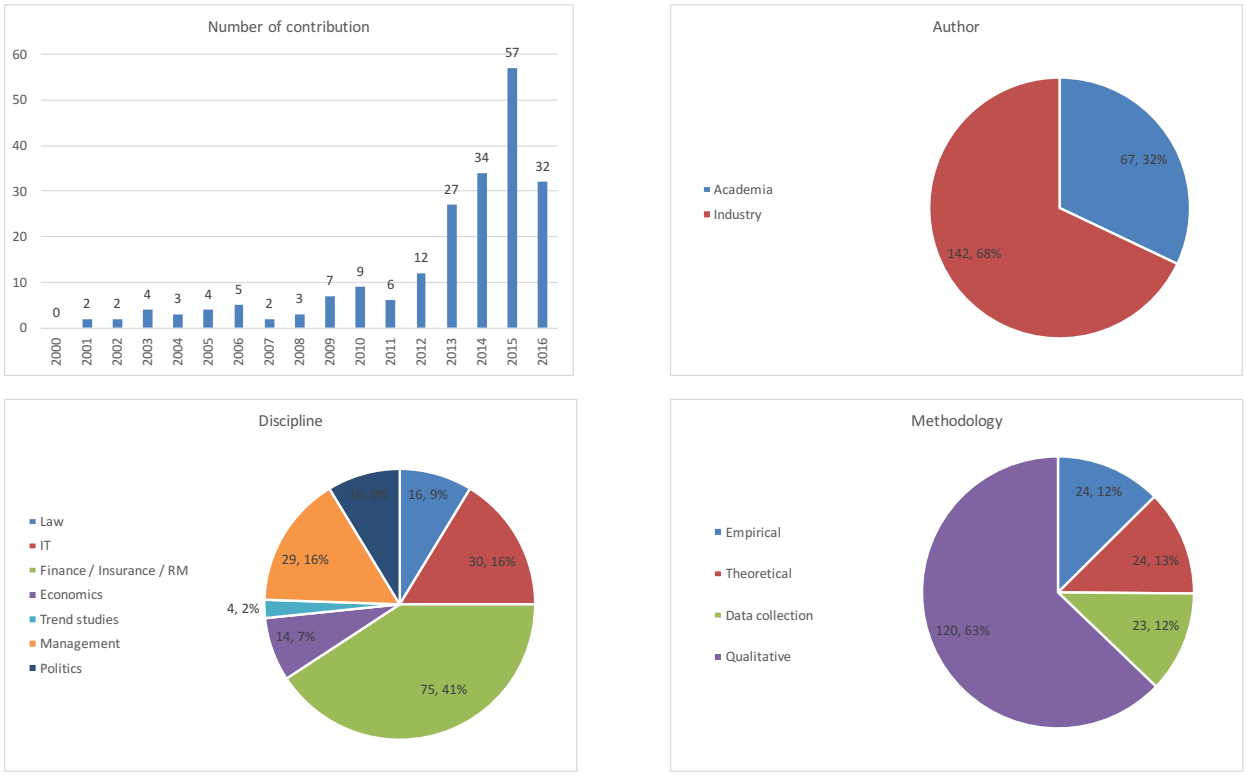
- Micro perspective: conduct more research on the demand side (e.g. risk perception, fatalism); analyse insurability and ways to improve insurability (especially empirical research, e.g. data generation, data, analysis); analyse optimal risk management (mitigation vs insurance) and how much capital is needed to cover cyber risks.
- Macro perspective: conduct more scenarios analyses for measurement and management of accumulation risk, analyse whether insurance companies can become a systemic risk with cyber insurance, become part of the global dialogue with stakeholders.

2. Methodology

We implemented our research in three stages: first, we conducted a review on 'cyber risk' and 'cyber risk insurance' using a standardised search and identification process described in Appendix B. Secondly, we discussed the review results with certain Geneva Association Members' companies and, in this context, also provided a platform for studies to be added. Based upon this result, a database was set up and the main research findings extracted.

In Appendix C, we have structured 211 papers by year, author (academic, industry), discipline (law, IT, finance / insurance / risk management, economics, trend studies, management, politics), and methodology (empirical, theoretical, data collection, qualitative). We have also classified the studies within the risk management process (risk identification, assessment, management (mitigation/ insurance), monitoring, and management in a broad sense) and used a set of selected key words.[4] Figure 2 presents descriptive statistics on the research results. The review contains papers published between January 2000 and May 2016.

Figure 2: Descriptive statistics on the review results



4 The keywords are amongst others: systemic cyber risk; operational cyber risk; underwriting cyber risk; man-made (cybercrime, denial of service (DoS), data breach); act of nature; risk modelling; asymmetric information; cyber insurance; regulation; accumulation risk.

3. Summary of Existing Knowledge on Cyber Risk and Cyber Insurance

3.1 What is cyber risk? Definition and categorisation

- Any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology (OT) eventually leads to business disruption, (critical) infrastructure break down, and physical damage to humans and properties.

- Cyber risk is either caused by natural disasters (e.g. floodings or earthquakes) or is man-made where the latter can emerge from human failure, cyber criminality (e.g. extortion, fraud), cyberwar, or cyber terrorism. It is characterised by interdependencies, potential extreme events, high uncertainty with respect to data and modelling approaches, and the risk of change.

While the extensive use of IT has increased quality of life and economic prosperity, it has also created new types of threats and increased the vulnerability of modern society. However, as awareness is increasing and cyber risk is being broadly discussed in academia and the mainstream media, it is not always clear what exactly is meant by this term. Here, we scan all references from our literature review for different approaches to defining cyber risk and systematically compare them (see Appendix D). Since our focus is cyber risk from an insurance perspective, we will advocate a definition that comprises all risks that show similar characteristics (e.g. with respect to distribution, correlation, mitigation instruments) in order to facilitate the modelling and management of such risks.

In general, cyber risk can be categorized according to several dimensions. The most obvious approach would be to differentiate between man-made threats and such caused by natural disasters. For example, floodings, earthquake and fire alike can cause physical damage to IT infrastructure such as servers and networks. On the other hand, man-made cyber risk can be classified according to the activity (criminal, non-criminal, intentional, accidental), the type of attack (e.g. malware, insider attack, spam, DoS, botnet, hard- or software failure) or the source (e.g. terrorists, criminals, governments). The attacks depend mainly on the activity and are reinforced by network effects (e.g. worms). The vulnerability of the company then determines whether an attack is successful. As the **vulnerability** is determined to some extent by organisation-specific parameters such as technology, processes, and people, it is characterised by an idiosyncratic risk component, which, for an insurer, poses the risk of moral hazard. Due to the public-good character of IT security investments, i.e. the security level of a company depends on the security measures of other partners in the supply chain, companies tend to invest less than what would be optimal for society (Biener, Eling and Wirfs, 2015). Finally, regarding the **consequences**, depending on the aim of the attackers (e.g. espionage, sabotage, extortion, exploiting information), the attack might compromise the availability of IT services, and the integrity and confidentially of data, which in turn leads to monetary loss, be it reputational damage or business interruption (see CRO Forum, 2014) or even damage to humans.

The term **cyber** has **two constitutive elements**, i.e. it relates to electronic communication **networks** and **virtual reality**. Both characteristics distinguish cyber risk fundamentally from other types of risks. Firstly, the virtual reality emphasises the intangible nature of, and therefore, the difficulties in assessing the losses. Secondly, networks are closely connected to the term cyberspace, which is frequently used synonymously with the Internet. While the Internet might be the main source of cyber threats (due to its public domain), cyberspace describes more generally every network that connects IT systems (e.g. LAN, WAN). For example, Refsdal *et al*. (2015) define cyberspace from a rather technical perspective as '[…] a collection of interconnected computerised networks, including services, computer systems, embedded processors, and controllers, as well as information in storage or transit.' Following that definition, they eventually define cyber risk recursively as exploitation of cyberspace. Clearly, this definition would not contain purely local incidents such as damage to a server due to flooding. Instead, as the term 'network' is constitutive, it emphasises the very nature of cyber risks, such as interdependencies, global scope, location independency and complexity. These characteristics are of importance since they can give rise to instability and systemic risk. Helbing (2013) analyses the behaviour of

such systems and argues that only small local changes can cascade and be reinforced throughout the whole network. Moreover, even if every component of a network taken by itself is safe, the interaction of several components can lead to instability and catastrophic events. Several other researchers use definitions that emphasise the significance of networks (Swiss Re, 2014; CRO Forum, 2014; Lloyd's, 2015; Willis, 2013).

In comparison, other authors do not stress the term 'network' explicitly as constitutive and use **broader definitions**. For example, Cebula and Young (2010) define it as 'operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems'. Similarly, the National Association of Insurance Commissioners (2013) list identity theft, disclosure of sensitive information and business interruption as examples of cyber risk. Other researchers investigate **only one particular type** of cyber risk such as data breaches (Böhme and Kataria, 2006). Thus, they all concentrate more on the potential negative consequences and the value at risk. Others see the **motivation of the attacker** as relevant. For example, Mukhopadhyay *et al*. (2005, 2013) concentrate only on malicious events. Related to that is also the terms 'cybercrime' or 'cyber-attack'. Kshetri (2010), for example, defines cybercrime as 'a criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules or regulations.' Indeed, a major subset of cyber risks is threats caused by cybercrime (73.9 per cent according to Hackmageddon, 2016). A large amount of the literature investigates the motivation and incentives of cyber criminals. For example, Kshetri (2010) analyses the potential benefits and costs a criminal can generate by conducting an attack.

A special type of cybercrime that shows specific characteristics is **cyber terrorism**. While terrorist and hackers use the same toolkits (e.g. DoS), their motivation is different and so is their potential target and their intended damage. As cyber criminals are motivated by the potential financial gain, curiosity, peer recognition or addiction, the cyber terrorists' intention is to damage their enemy and create fear, panic, and chaos. Therefore, of special interest for terrorists are systems that control a society's critical infrastructure such as power plants and traffic management systems. Although these systems tend to be well protected, they are vulnerable to terrorist attacks. As terrorists usually possess more resources than hackers, their attacks are more sophisticated, and they are able to maintain them for a longer period if required (Hua and Bapna, 2013). Moreover, government measures to deter them with severe punishment might not be very efficient, as their ideological reward founded in religion might overcompensate the potential adverse effects (Hua and Bapna, 2013). Whether a cyber incident is a terrorist act can be important since for example the U.S. Terrorism Risk Insurance Act provides insurers with a governmental backstop.

Cyber risk can also appear in the form of cyberwar where a hostile nation attacks the IT infrastructure of another nation. Targets could potentially be the government's IT system in an attempt to get access to sensitive information or it could aim at critical infrastructure. Examples are the DoS attack in 2007 on governmental institutions in Estonia, the Stuxnet virus used to harm nuclear facilities in Iran in 2010, espionage, manipulation and DoS attacks that came along with the Arab spring in 2011, as well as disclosure of NSA data by Edward Snowden in 2013 (see Biener, Eling, Matt and Wirfs, 2015). **Cyberwar** is fundamentally different from traditional war. Even a small country can dare to harm a bigger one, and the time and place of attacks are unpredictable (Clarke and Knake, 2015). Clarke and Knake emphasise that cyberwar enables strikes that are possible with conventional methods such as poison gas emissions from chemical plants, metro derailments, aircraft collisions, nuclear plant shutdowns and the blocking of traffic. From an insurance perspective it is important to note that losses due to an act of war are usually not covered but in practice it might not be possible to determine whether an attack is indeed an act of war or something else.

Another relevant aspect is that cyber risk can affect insurance companies in two fundamentally different ways. Firstly, since an insurance company relies critically on its IT infrastructure, it is highly vulnerable to cyber risk. This exposure is treated by regulatory frameworks as part of the operational risk category (**operational cyber risk**). Secondly, writing cyber risk policies seems to be an attractive business opportunity for insurance companies in an otherwise quite saturated market (**underwriting**

cyber risk). Additionally, from an insurance perspective, the distinction between **IT** and **operational technology** (OT) cyber risk is of importance (Lloyd's (2015b)). While both threats emanate from cyber space, they negatively affect different assets. On the one hand, IT cyber risk is the potential violation of data and systems integrity. These assets might only be insured by dedicated cyber policies. On the other hand, OT risk refers to a situation where the underlying processes, (critical) infrastructures and supply chains are affected (including physical damages). Depending on the terms of the policy, conventional (non-cyber), policies, such as general liability, might cover OT, but usually not IT cyber risk (see Section 3.7 for a more detailed discussion). It also should be noted that IT and OT (or alternatively the digital world and the physical world) are more and more converging, e.g. with the development of the Internet of Things.

It has to be emphasised that cyber risk might differs from other common risk. While most insurers have historically provided protection mainly for less correlated risk (e.g. motor insurance), cyber risks might be stronger correlated (e.g. Ögüt *et al*. 2011). The global interconnection of different IT systems causes geographical boundaries to vanish. Moreover, as the production of IT systems is characterised by significant economies of scale, the variety of products in the market is limited. Thus, if a security leak is spotted, it can be exploited in a multitude of systems. This homogeneity even applies to systems that should provide IT security (e.g. antivirus software). Global interconnection also makes it more difficult to curtail cyber risk. Eling and Wirfs (2016a) describe the main characteristics of cyber risk as follows: they are highly correlated, global, result in first- and third-party losses, and can be short tail and long tail. Eling and Wirfs (2016a) also distinguish among the 'cyber risks of daily life' (such as the usual hacker attack on a single company), which are insurable today; more problematic, however, is the risk of extreme scenarios, where cyber losses are not independent (leading to potential accumulation of risk). Another uniqueness of cyber risk is the risk of change. New technologies and regulations continuously affect the nature cyber risk. Finally, mitigation instruments are of high importance; in addition, there is high moral hazard that comes along with selling insurance.

3.2 What are the costs and detrimental effect caused by cyber risk?

- Estimates for the costs caused by cyber risk vary substantially and different estimates include different costs types.
- The estimates of the global costs are enormous (up to 1000 billion USD per year).
- Most estimates are provided by software and consultancy firms that might be biased.
- The manifold detrimental effects have been analysed, for example, by using event studies and scenario analyses. The major part of the effects are indirect costs (reputational damage, loss of trust, damage to operational technology).

Estimating the costs caused by cyber risk is difficult, as there is high uncertainty and no accepted source of information. The incentive of affected institutions not to communicate cyber risk incidents and limited notification requirements contribute their share to the information deficit. Some types of cybercrime may even cause no costs at all or cannot be quantifiable (e.g. spread of racism, mobbing, trading of illegal drugs). However, several industry contributions try to estimate overall costs, costs per incident, and cost per record of a data breach as illustrated in Table 2.

Table 2: Cyber crime cost estimates

GLOBAL COSTS (IN BILLION USD, PER ANNUM)	
Symantec (2013)	113
McAfee (2014)	445 (375-575)
Kshetri (2010)	100-1'000

COSTS PER INCIDENT (IN MILLION USD)	
Ponemon Institute (2015)	3.8
Geschonnek *et al.* (2013)	2.1
Kaspersky Lab (2013)	2.4

COST PER RECORD (IN USD)	
Symantec (2013)	298
Ponemon Institute (2015)	217
NetDiligence (2014)	956

COSTS BY COUNTRY (IN % OF GDP; MCAFEE; 2014)	
U.S.	0.64
China	0.63
Japan	0.02
Germany	1.60

The annual **global costs of cyber risk** are generally estimated to be above one hundred billion USD which, emphasises the economic significance of cyber risk. However, the estimates vary quite substantially, which has to some extent to do with the definition applied. While Symantec (2013) takes only direct costs into account, McAfee (2014) also incorporates indirect costs such as the reputational costs for the hacked company. The wide range provided by Kshetri (2010) is based on secondary literature and emphasises the severe uncertainty when it comes to estimating cyber risk costs. The costs per data breach a hacked company faces show less variation and are estimated to be between 2.1 to 3.8 million USD. Moreover, the loss of each record (e.g. credit card number) causes costs from 217 to 956 USD.

McAfee (2014) also provides estimates of the cyber risk costs for different countries. Again, the numbers show strong **variation between different countries**. When comparing cyber risk costs globally, one might expect more developed countries to have higher sensitivity to cyber risk threats, as their economies more strongly rely on IT. However, as the numbers show, the variation is still evident even when comparing different developed countries. For example, for the U.S., the costs are estimated to be 0.64 per cent of GDP; for Japan, however, they are estimated to be 0.02 per cent of GDP, and for Germany, an extreme 1.60 per cent of GDP. While such extreme differences do not seem plausible intuitively, it is difficult to say which part of the extreme variations illustrate real differences in the cyber activity (if any) and which part is due to differences in reporting. McAfee (2014) attributes this variation to different disclosure procedures. Especially disclosure and other IT security regulations could affect the numbers. Overall, it seems that the existing cost estimates are far from perfect. These numbers also have to be interpreted with caution, as most of them have been estimated by potentially biased security and consulting firms. Anderson *et al.* (2013) discuss methodological flaws of such estimates and suggest an improved alternative, which, however, in aggregate also yields a number in the hundreds of billions of U.S. dollars.[5]

Anderson *et al.* (2013) argue that the major part of cyber costs are **indirect losses** (loss of trust—not attributable to an individual victim) and defence costs (e.g. antivirus software, insurance) rather than direct losses (e.g. theft of money). According to Anderson *et al.* (2013), the cyber criminals' earnings are roughly equal to the direct costs only. While the direct costs may simply be a (illegal) redistribution of wealth, the indirect and defence costs could mean inefficiency and a **welfare loss** for all of society. However, another question is whether the overall efficiency gains (lower transaction costs, economies of scale) brought by information and communication technology (ICT) outweigh the costs caused by cyber

5 The authors, however, explicitly say that an aggregation is not really meaningful.

risk. In collaboration with Zürich (2015), the University of Denver estimated the overall benefits and costs of the ICT.[6] Due to increasing interconnectedness, heavy dependency on ICT, and government-imposed restrictions on the Internet, the authors expect a deterioration of cyber security, and increasing costs and reductions in benefits. However, despite this trend, their projection states that the benefits will still outweigh the cyber risk costs by 2030, and they reckon in the year 2030, the net global benefit of ICT will be USD 160 trillion higher than the overall costs. Generally, it can be said that every new technology (e.g. cloud computing), while potentially increasing the efficiency (e.g. cloud computing), will come at a cost of higher vulnerability.

From a micro perspective, cyber risk can have severe consequences for companies, e.g. an insurer's clients. The total costs are potentially a combination of loss of profits, data breach, response costs, reputational damage, contractual damages, and extortion costs. Several studies investigate the effects cyber risk incidents have on companies' stock prices. For example, Cavusoglu *et al*. (2004) show in an event study that a **security breach negatively affects a company's stock price**. They estimate the loss to be as high as 2.1 per cent of the market volume or 1.65 billion USD per security breach.[7] A major part of the discount is explained by the reputational damage (Sinanaj and Muntermann, 2013). On the contrary, Campbell *et al*. (2003) as well as Hovav and Arcy (2003) find only limited evidence that data breaches or DoS attacks negatively influence the company's stock price. However, Campbell *et al*. (2003) provide evidence that a breach of confidential data has a larger negative effect on the stock price than a beach of non-classified information would have; Hovav and Arcy (2003) show a negative price effect for companies with a business model that is heavily based on the Internet. Thus, the markets seem to behave rationally, as the discount is proportional to the expected loss associated with different data. Besides the sensitive customer data of a company, intellectual property such as copyrights, trademarks, industrial designs and patents also might be at stake. It is important to notice that the theft of intellectual property can also hinder innovation, research, development and production of the overall society in the long run. It has been reported that the **rating agencies** are planning to take a closer look at companies' cyber exposures (e.g. Moody's, 2015; Standard & Poor's, 2015). More specifically, Fitch Ratings (2016) recently warned that it will downgrade insurance companies that write standalone cyber policies too aggressively because of the high uncertainty this line of business contains.

Moreover, Standard & Poor's emphasises that, because of the high uncertainty, insurers should not rely too heavily on statistical models but should instead set low coverage limits and stipulate strict exclusions in their cyber policies (Krieger, 2015).

For individuals, the leakage of personal data is a major threat not only because of the potential financial losses but also because of the social consequence and the 'loss of control'. This problem is intensified by the ongoing leakages leading to an **accumulation of personal**[8] **data** and information about vulnerabilities of potential targets in the hands of criminals (black markets; see Ablon *et al*., 2014). Using sophisticated data analysis techniques, criminals can reconstruct the individuals' identity with only very little information. For example, de Montjoye *et al*. (2015) show that with only four observations about time and place of credit card use, 90 per cent of individuals (out of 1.1 million) can be uniquely identified. In conjunction with publicly available data via social media, these trends are expected to lead to an ongoing **erosion of privacy** (Wheatley *et al*., 2016). A growing threat for individuals is also cyber extortion and cyber mobbing.

6 Zurich (2015) estimates that the benefits, such as a direct contribution to GDP, productivity gains, and benefits to consumers, to be 10 per cent of global GDP. The costs are composed of direct losses caused by the incident, opportunity costs, and investments in ICT security.

7 Interestingly, Cavusoglu *et al*. (2004) also show that stock prices of information security providers increase on average in value by 1.36% or 1.06 billion USD after the announcement of another company's security breach.

8 Clearly, after a data breach, the victim might be able to take some precautions (e.g. changing passwords). However, some information (e.g. addresses) cannot easily be changed and indeed, accumulate in the hands of criminals.

3.3 Where do we find data on cyber risk?

- Data on cyber risk is scarce, e.g. because the victims are reluctant to report such events.
- Most empirical papers on cyber risk rely on data breach information (not loss information), but recently, first loss databases have been set up (NetDiligence in the U.S.; Biener, Eling and Wirfs (2015) globally).

The **availability of data** on cyber risk is rather **scarce**. This might be due to the fact that institutions that have been compromised do not disclose incidents (Symantec, 2016). However, since 2002, U.S. entities that experienced security breaches are required to report the incident to their customer and other parties (National Conference of State Legislatures, 2015), which enhanced data availability. But even if historical data are available, the **fast changing environment** for cyber risk might render this data useless (CRO Forum, 2014). Some sources for aggregated cyber risk statistics have already been discussed in the previous section. In Panel A of Table 3 overleaf, we list all sources for aggregated data that are surveyed by the industry.

Since the studies reviewed in Panel A only report aggregated statistics, their value for modelling cyber risk better is limited. The most useful data for modelling would be the claims an insurer actually faces as recorded by NetDiligence (2014). In Panel B of Table 3, we list additional alternative sources of **raw data** potentially suitable for **actuarial modelling**.

Table 3: Data Sources

Source	Description
Panel A: Aggregated Data	
Cyber Attacks Timeline Master Index (Hackmageddon, 2016)	Collection of information about author, target, type and country of publicly reported cyber-attacks (regularly updated).
2015 Cost of Data Breach Study (Ponemon Institute)	Survey among 350 companies in 11 countries about the total costs of data breach and the costs per each breached item (sponsored by IBM; updated annually).
2015 Global Cost of Cybercrime Study (Ponemon Institute, 2015)	Survey among 252 companies in several countries about the costs caused by cybercrime (sponsored by HP; updated annually)
Cyber Claims Study (NetDiligence, 2014)	Survey among major cyber risk insurers on claims payed out (117 in total, most of them for data breaches). Additionally they record the number of breached records per incident, the type of cost covered by the policy (e.g. crisis services, legal defence), the type of data exposed (e.g. personal, health and financial information) and the cause for the data breach (e.g. Hacker, Malware).
eRiskHub (by NetDiligence) [9]	NetDiligence is currently setting up a proprietary database where the anonymised data from all cyber claims studies are accessible.
Internet Security Threat Report, Norton Cybercrime Report (Symantec, 2016)	Recorded data are based on attack sensors placed all over the world. Moreover, the company maintains a database on vulnerabilities.
Net Losses—Estimating the Global Cost of Cybercrime (McAfee, 2015)	Estimates the global loss data based on several data sources (e.g. German Office for the Protection of the Constitution, the Netherlands Organisation for Applied Scientific Research (TNO), China's Peoples Public Security University, the European Commission, the Australian Institute of Criminology Research, and estimates by government agencies in other countries and consulting and cybersecurity companies around the world.)
ICSA survey (by ICSA Lab)	Survey among 300 companies on the infection rate by malicious codes and the associated costs (used by Herath and Herath, 2011).
Data Breach Investigations Report (Verizon, 2016)	Data on over 100,000 cyber risk incidents (incl. data breaches) for several countries contributed by security service providers, law enforcement, and government agencies.
Panel B: Raw Data	
Biener, Eling and Wirfs (2015)	Extract cyber losses from a worldwide data set of publicly reported operational losses (SAS OpRisk Global Data[10]) using a predefined search algorithm.
DataLossDB (by Risk Based Security)[11]	Information on data breaches from 1995 until present including number of breached items per incident, involved organisations, data type and more (regularly updated, former open security foundation). Is considered as the most comprehensive source of information about data breach (used by Maillart and Sornette; 2010 and Wheatley *et al.*, 2016).
Chronology of Data Breaches (by privacy rights clearing house)[12]	Compiles publicly reported data breaches from 2005 until present collected by a U.S. based non-profit organisation. It contains information about type of data breach, involved organisations and the number of breached items per incident. 4,486 entries in total. (used by Edwards *et al.*, 2015).
National Vulnerability Database (by NIST)[13]	Collects software vulnerabilities for the U.S. (used by Maillart and Sornette; 2010).
Honeynet[14]	Honeypot projects (e.g. Leurre.com) conducted by Honeynet, an international non-profit organisation. The honeypot (software or server), simulates a potential target, registers the attacks and thereby measures malicious activity in the Internet (used by Böhme and Kataria, 2006).
Internet Storm Center (ISC, by SANS Institute) [15]	Collects daily number of attacks per origin and target country (sensors register the criminal activity at different places.).
Cyber Data set (by Advisen) [16]	Proprietary database on Cyber risk related events such as data and system breaches and security violations.

9 https://eriskhub.com, last accessed 5 May 2016.
10 https://www.sas.com/content/dam/SAS/en_us/doc/productbrief/sas-oprisk-global-data-101187.pdf, last accessed 5 May 2016.
11 http://datalossdb.org/primary_sources, last accessed 5 May, 2016. Since 2015 the data base is provided by Risk Based Security (RBS): https://www.riskbasedsecurity.com.
12 https://www.privacyrights.org/data-breach, last accessed 5 May, 2016.
13 National Institute of Standards and Technology (NIST): https://web.nvd.nist.gov/view/vuln/search-results?query=&search_type=all&cves=on, last accessed 5 May 2016. http://www.us-cert.gov/cve.html
14 https://www.honeynet.org, last accessed 5 May 2016.
15 https://isc.sans.edu, last accessed 13 May 2016.
16 http://www.advisenltd.com/analytics/advisens-cyber-data set, 13 May 2016. Currently there is a growing number of specialised consulting firms that offer insurance companies data on cyber risk via web monitoring techniques.

3.4. How can we model cyber risks?

- Frequency and severity modelling of cyber risk can be done by applying extreme value theory and the peaks over threshold approach. Heavy tail distributions have been proposed, i.e. the power law or the log-normal distribution for the severity and negative binomial distribution for the frequency.

- The aggregation of cyber risk needs to take nonlinear dependence into account (typically applying copulas). The few existing modelling papers emphasise the immense modelling difficulties and risk of change. Scenario analysis is a popular tool in such situations

Due to the poor quality of data and the fast changing risk landscape, there is no established method to model cyber risk, and not much research has been done so far. The poor quality of data required insurers to analyse cyber risk from a technical rather than a statistical point of view. It has also been proposed to rely stronger on scenario approaches (e.g. Lloyd's, 2015b). Rakes, Deane and Rees (2012) argue that, especially for sparse but high-impact IT security breaches, it might be better to rely on an expert's judgement in defining worst-case scenarios and their likelihood. Focusing primarily on the risk accumulation in an insurer's portfolio and extreme events, RMS (2016) also proposes a scenario approach;[17] they define scenarios such as cyber data exfiltration, a DoS attack, compromising of financial transactions, cloud provider failure, and extortion. The risk accumulation is simulated by letting extreme scenarios influence all exposures in a portfolio labelled with the same attributes (see the data scheme of CCRS (2016) and Section 4).

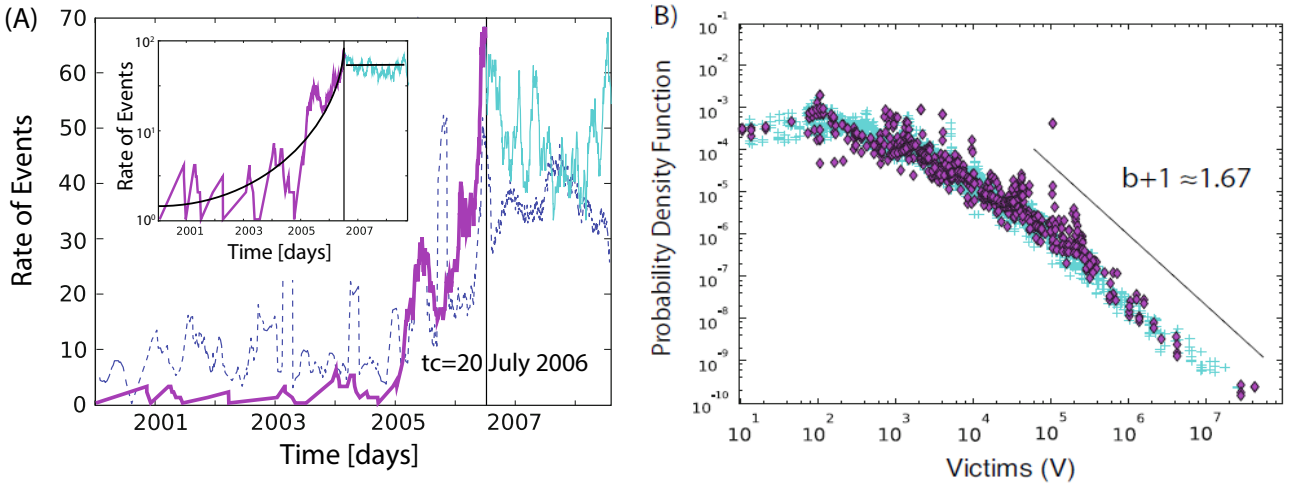
The approach allows for interdependencies between cyber policies written by different clients as well as between cyber and conventional policies. This framework provides a guideline for insurers to better diversify their overall cyber risk exposure geographically, business sector and size, cyber threat category, and ratings of a client's IT security level.

However, Maillart and Sornette (2010) investigate personal **data breaches** such as credit card, social security numbers, banking accounts or medical files. They find that the frequency of such incidents (rate of events) have been (faster than) exponentially growing in the period from 2001 to 2006 (Figure 3A overleaf). However, it seems that by 2006 the development plateaued out. Moreover, Maillart and Sornette (2010) find that the severity (number of breaches) per incident has an extremely **heavy-tailed-distribution** (Pareto index of 0.7) and the laws governing its distribution have been stable over time. This empirical distribution function is illustrated in Figure 3B overleaf where the violet dots are the observations before 2006, and the blue dots the observations after that date. While personal data breaches are only one type of cyber risk, the authors argue that these findings are representative for other types of cyber risks originated in the Internet.

Building on this work, but with an up-to-date and broader data set, Wheatley *et al*. (2016) conduct a similar analysis and find that the amount of breached items per incident have had an even more heavy-tailed distribution since 2007 (Pareto index of 0.37 for 2015) and the breach size is expected to double in the next five years from an estimated 2 billion personal items to 4 billion.

17 Risk Management Solutions (RMS) is one of the large catastrophe modelling agencies and they also provide solutions for cyber risk insurers. Other catastrophe modelling agencies are starting to offer services in the cyber risk field (see, AIR Worldwide, 2016; Cyence).

Figure 3: Frequency and severity distribution (Maillart and Sornette, 2010)



The results show that the laws governing the properties of cyber risk, be it the frequency or severity, are highly dynamic. The **fast changing technology environment** requires continuous revisions of modelling approaches. Moreover, the quality of available data limits the improvements in modelling that can be made. Especially for insurance purposes, a pure number of data breaches is not sufficient when calculating premiums, capital or reserves. Instead, a price tag corresponding to the potential claim has to be allocated to each data breach. Finally, classical risk measures based on mean and variance might fail to be applicable, and the merits of diversification might vanish due to the infinite moments that characterise cyber risks (see Chavez-Demoulin *et al*., 2006).

Similarly, Edwards *et al*. (2015) investigate trends in data breaches between 2006 and 2015. However, they find no evidence for an increasing trend in frequency or in severity (number of records per incident). They argue that the widespread intuition that the frequency and severity of data breaches are increasing, might be just an artefact of heavy-tailed loss distributions (while severity is best described by the log-normal distribution, the frequency follows a negative binomial distribution). Moreover, Edwards *et al*. (2015) use the estimated cost per record as provided by the Ponemon Institute (2014, refer to Section 3.2) in order to estimate the overall costs of data breaches in the U.S. The researchers estimate the cumulative cost to be between 3 and 55 billion USD for the next three years.

Besides modelling the marginal distribution of cyber risks, the second challenge is aggregating them, especially when they are correlated, as is the case with cyber risk. Indeed, correlation of cyber risks has been discussed as being detrimental to the development of a cyber insurance market. Böhme and Kataria (2006) systematically investigate correlations on two levels. Firstly, an event could affect several systems within a single entity (e.g. company). Secondly, there is correlation across different entities (e.g. an insurer's portfolio of policies). Different types of risk might be characterised by different correlations (see Table 4).

Table 4: Correlation types (Böhme and Kataria, 2006)

		GLOBAL CORRELATION	
		Low	**High**
INTERNAL CORRELATION	**High**	Insider attack	Worms and viruses
	Low	Hardware failure	Spyware/ phishing

The authors build a model that shows that insurance is especially suited for risks that show high **internal and low global correlation**. The reason for this is that low internal correlation would allow the company to eliminate the risk by self-protection more efficiently. Moreover, a high global correlation is detrimental to the insurer's diversification merits and would drive the charged premium up. The authors suggest that increasing diversity of the system platforms could reduce internal and external correlation. For example, governments could use competition laws to increase the diversity of available software products. However, that approach could also reduce compatibility between different systems and lower the economy of scale in the production process.

Due to rather **complex dependencies**, aggregation of cyber risk (of e.g. a portfolio) can be quite challenging. Using copulas has the advantage that they allow for any potential marginal distribution (what might be especially helpful for the diverse cyber risk class) and account for non-linear dependencies. Böhme and Kataria (2006) suggest the t-copula, as it is suitable to model the correlation of extreme events. However, they employed the t-copula purely for simulation exercises and emphasise that better data would be required in order to estimate suitable copulas and parameters empirically. However, they also conducted empirical tests and estimate a correlation coefficient for global attacks (see Table 5) of only 0.03 and 0.18 depending on the model applied. Moreover, their estimates for the internal correlation coefficient is smaller than 0.1. Herath

Table 5: Comparison of different modelling approaches

	Level	Frequency	Severity	Dependency	Modelling approach
Panel A: Modelling of Correlations					
Mukhopadhyay *et al.* (2013)	Company	Number of failures	Costs given loss	Gaussian copula	Copula aided Bayesian belief networks
Böhme and Kataria (2006)	Company / portfolio	Number of attacks (beta binomial)	-	Company: linear portfolio: t-copula	Dependent Bernoulli trials -> Beta binomial Source of correlation: attacks
Böhme (2005)	Portfolio	Number of claims (binomial)	-	Linear correlation (frequency)	Correlation due to a few IT system providers (concentrated market)
Panel B: Total Loss Modelling					
Herath and Herath (2011)	Company	Number of affected computers	Loss per affected computer	Archimedean copulas (Clayton, Gumbel)	Modelling the dependency between number and amount of losses.
Maillart and Sornette (2010)	Global	Number of data breaches	Number of records per data breach	Non	Estimating a linear model for severity and frequency distributing
Edwards *et al.* (2015)	Global	Number of data breaches	Number of records per data breach (& costs per breached record)	Non	Estimating a linear model for severity and frequency distribution
Wang, Q.-H., Kim, S.-H. (2009)	Global			Partial correlation (2009)	Estimate the correlation of cyberattacks between countries.
Eling and Wirfs (2015)	Global		Losses per incident	None	Extreme value theory (point over threshold)

and Herath (2011) analyse losses due to virus incidents and find that the marginal distributions are not normal, and the risks are correlated in a non-linear fashion. As a remedy, the authors suggest using Archimedean copulas (Clayton and Gumbel) and conducted simulation exercises. Mukhopadhyay *et al*. (2013) use the normal copula in order to aggregate the number of failures (frequency) and the loss given default (severity) in order to derive the overall loss distribution on a cyber risk portfolio. To conclude, as more data on cyber risk become available, research should be aimed at improving the understanding and modelling techniques of the rather complex interdependent cyber risk.

For the modelling of **interdependencies** in threats emanating from the Internet, the network's characteristics and the type of threats are important. The relevant network for modelling the risks is not necessarily identical to the physical network. Instead, it might describe a network created by social media or email services. On the one hand, malicious codes (e.g. virus) seem to propagate in a way similar to the spread of pandemics (Bolot and Lelarge, 2009). Highly interconnected (dense) and low clustering networks provide an optimal environment for the spreading of malicious code. On the other hand, a local destruction of physical components, such as the breakdown of a submarine cable, will have more severe effects if the Internet's topology has low density and high clustering. Thus, the same network properties can potentially increase the vulnerability to one threat and simultaneously enhance resilience to another one. As it is usually assumed that the Internet is a rather decentralised and dense network (e.g. Ahamad, 2012), pandemic-like attacks pose a bigger threat than to the local destruction of physical components (see Section 3.6)

3.5. Micro perspective: How should cyber risk management be organised?

- There are special standards and tools for cyber risk management. In each step of the classical risk management process (identification, evaluation, management, and monitoring), cyber risks show special features.
- Institutional commitment, effective crisis management, risk communication with employees, customers and suppliers, and continuous monitoring are fundamental. Cyber risk management today focuses on risk mitigation, while the risk transfer so far plays only a minor role.

The classical risk management process consists of five steps: the definition of goals, risk identification, risk evaluation/analysis, the actual risk management (avoidance, mitigation, transfer, retention) and finally, the monitoring of risk. In each step of the classical risk management process, cyber risks show special characteristics. The first and maybe most important aspect for sound cyber risk management is that cyber risk management is not the responsibility of the IT department, but a cross-company risk dialogue is necessary (e.g. sensitisation, trainings etc.). The topic also should be embedded at the C-level.[18] Already the institutional commitment—demonstrated by having a person responsible for information security—is essential for a successful management of the risks category. For instance, firms with a chief information security officer (CISO) or a similar position installed, have lower average cost when a breach occurs (USD 157 per record vs USD 236 per record for firms without strategic security leadership; see Shackelford, 2012).

The first step in the risk management process is the definition of the **initial situation and goals** of the cyber risk management. By now, there exist a multitude of industry standards, in particular from the field of information technologies, which can serve as templates for cyber risk management, for instance, the family of ISO/IEC 2700x standards, the BSI-IT-Grundschutz (BSI, 2008), or the Cyber Security Best Practices (Allianz, 2011). There exists also the opportunity to certify compliance with such standards. For example, the U.K.'s Department for Business, Innovation & Skills and Cabinet Office (2014) defines, in the so-called Cyber Essentials scheme, an IT security standard and a certification of its implementation.[19] Business partners and customers increasingly require companies to verify that they fulfil certain minimum IT security standards. Especially, companies seeking cyber coverage would need to have such a certificate or the insurer would have to conduct a similar risk assessment itself. [20]

For the **risk identification**, assets with their corresponding business process that are relevant for the cyber risk management must be identified. Afterwards, potential threats, their type and potential sources must be determined. A detailed list of current threats is provided by ISO/IEC 27005. Ultimately, weaknesses, always with respect to assets, threats and already existing protection measures should be collected. A potential first indicator for risk identification can be provided by a cyber-risk self-assessment; e.g. by Marsh.[21] Those tools can help to determine the risk exposure, and the risk awareness of a company, and provide indications for which risks are not identified yet. Whether such tools will be broadly accepted remains an open issue. Another aspect would be how an attack can be detected as quickly as possible when it happens.

18 The step down of Target's CEO following a massive data breach in 2014 exemplifies that the top management might be held accountable for cyber incidents (http://www.forbes.com/sites/greatspeculations/2014/05/08/targets-ceo-steps-down-following-the-massive-data-breach-and-canadian-debacle/#799cf7283f56).

19 This certificate is required for companies in order to be admitted for public procurements. A similar framework is in place in Japan and a proprietary framework specifically tailored for the needs of SMEs is provided by VdS (2015). Moreover, there exist industry specific standards, e.g. Payment Card Industry Data Security Standard (PCI DSS) and NERC's Critical Infrastructure Protection (CIP).

20 ACGS (2014) analyses cyber risk management with the Business Model Canvas and the House of IT Quality.

21 See http://www.marsh-stresstest.eu/.

Risk analysis means that consequences, probabilities of occurrence and risk levels are estimated. A tool for the analysis of consequences for the business operations is the business impact analysis (BIA). First step in this method is the calculation of direct costs for particular scenarios. Via dependencies between different scenarios, the expected total loss of an incident can be estimated, thus both the direct costs and the indirect costs. For cyber risk is of particular interest, since consequences can be very diverse and are not restricted to pure recovery costs. The analysis has to incorporate also potential reputational effects, which might have a strong negative impact on the enterprise value.

The estimation of probabilities of occurrence is one of the biggest challenges in this part of the risk management process. Since cyber risk is a relatively new risk category, there are not many data available for an adequate estimation of probability. Furthermore, cyber risk is very dynamic, fast moving, and is subject to significant risk of change, which is why statements for the future, estimated by statistical surveys from the past, must be viewed with caution. [22]

For the actual **risk management** there exist four options to handle the risk: risk avoidance, risk reduction/mitigation, risk transfer or self-insurance. Risk avoidance would mean that the electronic storage of information and the use of information systems must be restricted. In the world of today, this is difficult to imagine. Risk reduction and mitigation seems to be more effective here. These are instruments to reduce the probability of occurrence (e.g. anti-virus software, firewalls etc.) or that mitigate the size of losses (e.g. emergency guidelines).[23] Deciding on what technical IT security measures should be taken to reduce or eliminate cyber risk exposures as efficiently as possible can be a difficult task. Rakes *et al*. (2012) point out that most companies do not have a sound decision-making process in place. Thus, they propose a framework where different countermeasures are compared, based on their suitability in reducing cyber risk threats. Formulated as an optimisation problem that accounts for cost, suitability, and budget constraints, this framework can help to select the most efficient means available.

In general, the transfer of risk is possible by the purchase of an insurance contract. Unfortunately, the access to cyber risk insurance solutions used to be limited and the available coverage limits were rather low. However, as the market for cyber insurance is developing, the product range will increase and higher coverage will become viable. Particularly important is also the combination of risk reduction/mitigation and transfer. An insurer will only write a policy if appropriate risk reduction/mitigation measures are in place and the insurer was able to verify the effectiveness of these tools in up-front assessments. Thus, up-front assessments and interviews are needed in advance of signing an insurance contract. These assessments will also help to increase the awareness for cyber risk. In case of self-insurance, the company decides to pay remaining losses on its own. For this case, the firm's equity capital must serve as a safety buffer and must be saved in advance. Besides the accumulation of equity capital, emergency guidelines must be established. An effective crisis management plan is an important prerequisite for dealing with cyber risk properly.

Because of the high dynamic, ongoing **risk monitoring** is a very important key in cyber risk management. The strategies of attacks change constantly. Thus, the risk management has to adjust permanently. In this context, thorough communication and information sharing is of high interest for cyber risk, not least because this reinforces security know-how and security awareness in the whole company. For a company to be able to react on developments appropriately, it has to adopt its risk management process constantly.

22 See also Office of the Superintendent of Financial Institutions (2013).

23 See CIS (2016) or ASD (2014) for guidance on how IT security measures, such as access control, authorisation of devices and software, malware defense, and network configuration, should be used.

In summary, we can derive the following guidelines for cyber risk management (see also Biener, Eling, Matt and Wirfs, 2015, for a more detailed discussion):[24]

1. Institutional commitment: someone from the C-level has to be responsible for cyber risk (e.g. the implementation of a CISO reduces the average costs of a data breach by more than 30 per cent (Shackelford, 2012)).

2. Effective crisis management: for specific risk scenarios, clearly defined operating plans and responsibilities must be present (e.g. what happens in case of a data breach?).

3. Risk dialogue with employees: cyber risk not just a task for one special department, but a cross-company risk dialogue is necessary (e.g. sensitisation, trainings etc.).

4. Risk dialogue with customers and suppliers: cyber risk also requires a permanent dialogue with customers and suppliers (how is their security level? › contagion).

5. Certification: if necessary, certification according to an information security standard can be an important signal for customers and suppliers. However, certification should not lead to a 'box-ticking-mentality'.

6. Continuous monitoring: because of rapid technological development, the risk management process needs to be adjusted constantly, since always-new sources of threat emerge. An efficient monitoring and verification process is imperative.

7. Risk transfer: insurance can be an effective means of transferring cyber risk.

Today's cyber risk management focuses on risk control and prevention (i.e. self-protection and self-insurance measures), while risk transfer plays no role or only a minor one. This leads to the question: How can we organise risk transfer for cyber risk? Section 3.7 will elaborate on this question in more detail.

24 It should be noted that especially small and medium-sized businesses (SMB) are vulnerable to cyber attacks. According to Symantec (2015, almost two-thirds of the attacks in 2014 were directed at SMB's, which might not be interesting to attackers in the first place, but could give a backdoor into other companies with more efficient security systems. SMB's with less resources are thus a gateway to larger and better-protected companies.

3.6. Macro perspective: Is cyber risk a threat to the global economy and society?

- A global failure of the Internet is rather unlikely, but regionally limited breakdowns have already occurred; given the globally connected economy and society, the potential consequences of such extreme scenarios on companies and individuals are massive.
- The same holds for other cyber scenarios such as, for example, the blackout of energy systems. For insurers such scenarios pose significant accumulation risk which will require detailed modelling

One of the most striking questions when it comes to discussing cyber risk is the extreme scenario of a breakdown of critical infrastructure, be it due to technical failure or to criminal activity. In theory, this could lead to massive economic losses (see, e.g. WEF, 2015) and to a breakdown of any cyber insurance market due to the huge accumulation risk. Numerous scenarios have been developed and widely discussed among both academics and practitioners (see, Ruffle *et al*., 2014).[25] But how likely is such an extreme event?

To the question of whether a total collapse of the Internet is possible, most experts respond 'no'. This assessment is usually justified by the topology or the general architecture of the Internet; it is highly decentralised, distributed over many servers and devices in different places and is very robust and resilient (see, e.g. Ahamad, 2012 or Beckstrom, 2012). In addition, the data are transmitted in various ways (mainly cable, but also satellites).

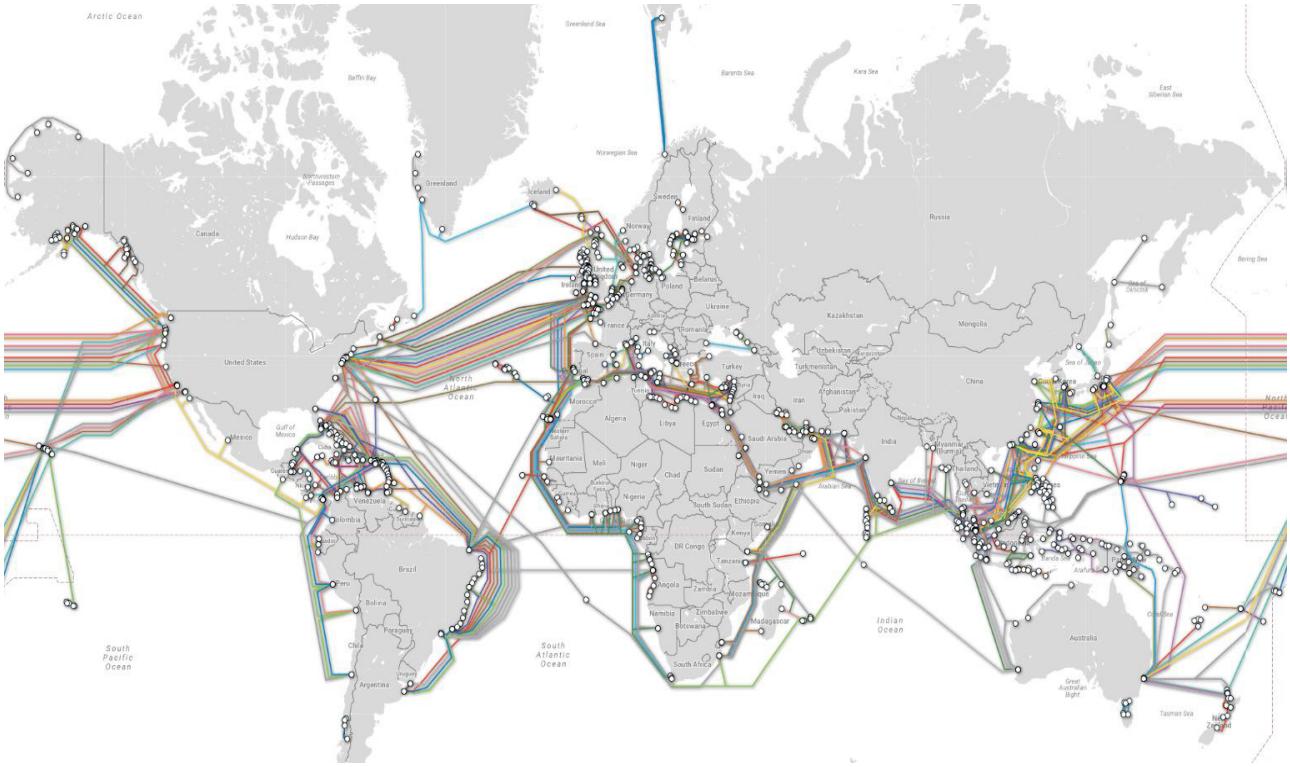
Although many experts are convinced that a (global) breakdown of the Internet is unlikely, the past has shown that large (regionally limited) breakdowns are possible. For instance, individual areas have been isolated from the Internet. For example, in March 2013 a cut of several submarine cables led to an incident in which almost the whole African continent was separated from the Internet for almost a day.[26] The exact cause is unclear, but it might be as simple as fishing nets that had become entangled in the cable. In most parts of Africa, not only the Internet was not functioning, but all transaction traffic was paralysed. During this time, it was impossible, for example, to perform foreign credit or ATM card transactions. It took a few days until all systems were error-free again (Hochstätter and Masiero, 2009). This illustrates that a break-down of the Internet can have a wide spread effect.

Figure 4 shows the laid submarine cables (as of February 2014). There are many parallel lines that are responsible for data exchange between the continents. Separating individual areas of the Internet may therefore indeed be possible, but a collapse of global data transmission seems rather unlikely in reality. According to Strickland (2010), there could, however, be other areas of concern for the Internet. Among these are damage to satellites and solar super storms, which again in turn would 'only' lead to a partial failure.

25 Worst case scenarios where IT systems, data, networks and services are affected on a large scale (e.g. critical infrastructures), are sometimes called 'Cybergeddon'. The scenario 'Cybergeddon' described by WEF (2014) features an unruly cyber space where attackers have gained the upper hand for good. Finally, these permanent disruptions would impair trust and individuals as well as organisations would seek to reduce their reliance on ICT.

26 A second example, which is going into the field of criminal activity, was the breakdown of the Korean Internet in December 2013. Recently, also the majority of the Swiss Internet for commercial use was interrupted for almost a full business day (on 24 May 2016) after a software failure.

Figure 4: System of submarine cables (TeleGeography, 2016)



Although the majority of experts considered the risk of total breakdown to be small, there are also opposing views on this. Recent research papers question the conventional wisdom that the Internet is robust due to its topology. Bashan *et al*. (2013) show in a network model that a failure of the Internet is well possible. Hochstätter and Masiero (2009) argue that especially IXPs (Internet Exchange Points, Internet nodes forming interfaces between different computer networks) are very vulnerable to attack from cyber-terrorists. Due to the dominant position of the router manufacturer for these IXPs, the Internet could even come to a standstill worldwide by attacking them in a larger region. Another danger can be seen in attacks on DNS[27] servers.

Although the data transfer over the Internet would still be guaranteed, targeted attacks could make it impossible to resolve domain names correctly, thus making the Internet useless.

In summary it can be said that a prolonged global failure of the Internet is considered as unlikely by most experts. But there is both theoretical and empirical evidence that at least partial failure of the Internet is possible. This is problematic as well, especially considering that there is relatively little contingency planning for such a scenario today. Although now many states have defined first national strategies to protect critical infrastructure, there is no real Plan B in case of a global failure. Companies and states should therefore discuss such a scenario in their emergency planning in greater depth.

27 Domain name system, the system that allows the resolution of Internet addresses.

These plans are also very important in light of the potential consequences of an extreme event like the breakdown of the Internet. For example, the World Economic Forum (2010) estimates that there is a 10 per cent probability of a critical information infrastructure breakdown within the next 10 years, with the financial consequences within the first few days alone amounting to about USD 250 billion. Such a scenario would stop all general communication such as text-messaging services or email. Cloud systems and online banking would no longer be available and the data stored on it would no longer be accessible (see Strickland, 2010). In addition, all websites would be offline, so that there would be no business anymore (e.g. with Amazon). In addition, the failure of the Internet could lead to far-reaching supply problems in industry. Manufacturing companies are increasingly connected with suppliers and customers via the Internet in order to enable efficient, just-in-time production (see Hochstätter and Masiero, 2009). In addition, it would not be possible to execute capital market transactions on exchanges and Internet platforms (see Hochstätter and Masiero, 2009).

Besides the supply bottlenecks, the failure of the Internet could also have an impact on households. Smart grids, transporting electricity or water, would no longer communicate and carry out their work (Strickland, 2010). Blackouts and undersupply would be possible. An extreme example is given by Ahamad (2012), who discusses a scenario where electronic medical records may not be available through lack of Internet, and so in the worst case, people may die. Lloyd's (2015b) describes a hypothetical, but not unrealistic (return period: 1:200-500) worst case scenario of a hostile cyberattack on the power grid serving 15 U.S. states. The study comprehensively analyses the wide spread consequences a cyber-attack (IT risk) would have as its effects cascade and finally damage physical assets (operational technology, OT risk). Besides the direct damage to the power grid, the failure of health and safety systems would increase mortality, the shutdown of ports, transport systems and communication would reduce economic activity, and the blackout of electric pumps would disrupt the water supply. Lloyd's (2015b) estimates the overall damage to be between USD 243 billion to USD 1 trillion. The insurance industry would face a variety of claims from several business lines from property damages to business interruptions (not necessarily cyber risk policies) and the accumulated claims are estimated to be between USD 21.4 billion to USD 71.4 billion. Kelly *et al*. (2016) draw a similar worst-case scenario for a cyber-attack on the UK. They estimate the overall cost, including a plunge in GDP, between GBP 49 billion and GBP 442 billion for the five years following the power outage. [28]

28 An alternative scenario where cyber risk could become a systemic threat is if widely applied soft- or hardware products are compromised. This could be the case if the global market for a certain business application is highly concentrated and business processes rely heavily on it. Building on experts' judgment, Ruffle *et al*. (2014) draw an extreme scenario where such a systemically relevant technology is compromised. They estimate that such a scenario is taking place once every one hundred years and the overall global loss is estimated between USD 4.5 trillion to USD 15 trillion. Moreover, they predict a plunge of the financial markets similarly to the financial crisis in 2008.

3.7. Cyber insurance market: What is the status quo and what are the main insurability challenges?

- The cyber insurance market is very small at present, but is expected to increase significantly in the coming years. The U.S. is far ahead Europe and Asia, for example, with regard to reporting requirements. However, forthcoming regulations in the European Union will probably level playing fields.
- Conventional policies (property and liability) are frequently silent on whether losses caused by cyber incidents are covered.
- The main insurability problems are the lack of data, risk of change, accumulation risk, loss sizes, availability of risk capital, and potential moral hazard problems.

Commercial property and liability insurance is available in most insurance markets worldwide.[29] However, most property policies only cover damage to physical assets such as production facilities and might exclude IT cyber risk, as is generally the case with liability policies. Often the terms of contract are even silent on what cyber events exactly would be included (Lloyd's, 2015b). While the customer might think that cyber incidents are covered, the insurer assumes that they are not. As this ambiguity might cause legal disputes, the judge's decision discretion and the legal costs increase the insurers' financial risk.[30]

As a consequence, insurers seek to state more explicit terms of contract in two ways. Either the insurer could adapt its policies by explicitly excluding them in traditional policies and providing dedicated policies (standalone cyber policy)[31] or it could explicitly include them and adjust the premiums accordingly (affirmative cyber policy). Behavioural insurance models, such as prospect-theory, could be employed in order to predict customers' perception of the two different options (separate new policies vs expanding existing policies) and provide a guideline (e.g. Schmidt *et al.*, 2008).

Recently, a specialised market providing coverage for cyber risks has emerged, most prominently in the U.S. As yet, however, market coverage is small. Moreover, outside the U.S., insurance coverage for cyber risk is not well known and little used. In Europe, for example, many corporations are not even aware that this type of insurance exists, and only very few have purchased cyber risk coverage (Marsh, 2013). Figures for the U.S. show a similarly low average level of coverage of about 6 per cent, but large variations between industries among the Fortune 1000 companies (Willis, 2013b).[32] According to Betterley (2015), current annual gross premiums for cyber insurance in the U.S. are USD 2.75 billion and growing 26–50 per cent on average per year. Advisen (2015) estimates the premium volume for the U.S. market in 2015 already to be in the neighbourhood of USD 2.4 billion. The premium volume in continental Europe is estimated to be around USD 192 million, but this figure is expected to reach USD 1.1 billion in 2018 (NAIC, 2013). Swiss Re expects an increase of the global cyber insurance premium volume to USD 5.9 billion by 2023 (Swiss Re, 2014).

29 Note that the majority of the discussion on cyber insurance refers to commercial insurance. Cyber insurance for retail customers is a new field with only few applications and examples. For this reason the majority of the discussion in this study focuses on the commercial insurance market.

30 A NY court ruled in 2014 in the case Zürich Insurance against Sony Corp. that general liability policies do not cover data breaches (http://www.insurancejournal.com/news/east/2014/03/17/323551.htm)

31 See London Institute clause 380, ISO Electronic Data Exclusion (2004) and Data Breach Exclusion (2014), NMA 2912, 2914, 2915 clauses (2001). This approach also has its limitations especially as the digital world and the physical world are more and more converging. See the discussion in Section 3.1 on information technology vs operational technology.

32 According to Willis (2013b), about 20% of all financial services companies have cyber risk coverage, whereas manufacturing (2%) and healthcare (1%) have the lowest share of companies covered. Another market survey for the U.S. by the Harvard Business Review Analytic Services (2013) finds that among 152 companies, market coverage is 19%.

Besides the low coverage of cyber risk in businesses, the market of cyber insurance for individuals is even less well-developed. There exist only very few personal cyber insurance products, and most people are not even aware of their existence. A study conducted by YouGov (2014) estimates that only one per cent of individuals possesses cyber insurance.[33] However, the potential for such products seems to be huge, as the survey finds that 19 per cent of the participants would be willing to buy such a product. The study does not survey what individuals would be willing to pay for cyber insurance.

In summary, the cyber insurance market is very small at present, but expected to increase significantly. The U.S. market is much more developed than its European counterpart, partly because the U.S. have had reporting requirements for cyberattacks in place for several years with relatively heavy fines for violations (SEC, 2016). [34] The new regulations have considerably increased the awareness of cyber risk and increased the demand especially for liability (third party) cyber coverage. The U.S. market is thus mainly dominated by third party coverage, whereas the few policies that already exist in Europe focus more on first party coverage. Now, however, discussions about the introduction of reporting obligations are taking place in the European Union. These new regulatory approaches might be an important driver in the development of the European cyber insurance market.

Owing to the new and evolving nature of the market, products and coverage change rapidly, and exclusions as well as terms and definitions vary significantly among competitors. Another distinctive aspect of cyber insurance is that the risks faced by corporations are often unique to a specific industry or even to the company itself, requiring a great deal of customisation in policy writing. Company size, size of the customer base, web presence and the type of data collected and stored are important determinants of cyber insurance policy terms and pricing. Typical cyber insurance policies in the third party field are privacy liability, network security liability, intellectual property, and media breaches.[35] First party coverages are in the field of crisis management, business interruption, data asset protection and cyber extortion.

Biener, Eling, and Wirfs (2015) discuss cyber risk beyond the background of Berliner's (1982) insurability criteria. The results outline the reasons for today's relatively small market. In the following, we discuss the three most problematic aspects of insurability. The first insurability problem is that the independence and predictability of losses is not given for cyber risk; thus, risk pooling might not always work appropriately. Pooling risks is further complicated by the fact that the risk pools for cyber risk are still small; the smaller the portfolio, the more difficult it is to achieve the full benefits of diversification. Another problem can be seen in the unpredictability of loss exposure, since losses are difficult to measure because of a lack of data. Moreover, even if there are data available, it is questionable whether or not historical data are a meaningful indicator for the future, due to the dynamic nature of cyber risks and thus the risk of change.

33 Generally, individuals not only buy less cyber risk coverage, but they also care less about IT security. YouGov (2014) finds that only half of all surveyed individuals have IT security measures in place.

34 See also the new regulatory initiative in NY that, among others, requires financial institution to notify the supervisor of any cyber incident, conducting a cyber risk assessment, and defining a cyber security policy (New York state department of financial services, 2016).

35 See, e.g. Marsh (2012). Sometimes, reputational losses (e.g. NAIC, 2013; Ponemon Institute, 2013) and regulatory fines (e.g. Betterley, 2013; Ponemon Institute, 2013) are also covered by cyber insurance policies.

A second significant problem in cyber insurance is information asymmetry. Companies that have experienced a serious cyber-attack are more likely to buy insurance (Shackelford, 2012), thus resulting in adverse selection. The insurers in the market try to alleviate adverse selection effects by screening (e.g. up-front audits), self-selection (e.g. questionnaires in the underwriting process), and signalling (e.g. certificates for IT-compliance). In addition, there is moral hazard (i.e. the change of behaviour after purchasing insurance). One example is the insured's lack of incentive to invest in self-protection measures following the purchase of insurance, if full coverage is offered. Insurers use instruments such as screening (e.g. audit) and risk sharing (e.g. deductibles, cover limits) to reduce moral hazard. Despite these manifold instruments, information asymmetries still pose a significant problem for the insurability of cyber risks. For instance, because of complex interrelations in modern IT systems, firms might be vulnerable to cyber risk even though they have invested in self-protection. Thus, the benefit of self-protection investments in one company highly depends on the investments in other, connected firms. This might amplify moral hazard problems, because incentives for self-protection might be reduced even further. In addition, the lack of loss data aggravates a risk-adequate classification of policyholders, thus exacerbating the adverse section problem. This problem might become less relevant when data resources increase.

A third essential problem for the development of an insurance market are coverage limits. Policies tend to cover only limited maximum losses (USD 10 to 500 million, see, Biener, Eling, Matt and Wirfs, 2015; Finkle, 2015), and contain several exclusions (e.g. self-inflicted losses, accessing unsecure websites, or terrorism). Potential extreme scenarios (sometimes called 'Cybergeddon'; see Section 3.6) can thus not be well covered by existing insurance policies. Additionally, there might be indirect effects of cyber losses that cannot be measured and thus are not covered (e.g. reputational losses and their impact on stock prices). Another problematic aspect of coverage limits is the complexity of the policy. Given the large number of exclusions and the dynamic nature of cyber risk, there is uncertainty about what the cyber policy actually covers. Worse yet, the policies in the market have no agreed-upon terminology, which makes the offerings very difficult to compare. Whether the cover limits are the result of a shortage on the supply side or insufficient demand is an open question.

Numerous problems with the insurability of cyber risk impede the development of a cyber insurance market. At the same time, we need to consider the time dimension. Today the cyber insurance market is in its early stages, but as market development continues, the risk pools will become larger and more data will be available. Several new competitors have entered the market and more are planning to do so. This will increase insurance capacity, competition and push prices down. Additionally, it will lead to a more uniform terminology and standardisation of products[36]. In light of our discussion, it might be also important to establish standards with regard to definitions, coverages and pre-coverage risk assessment, all of which will help to reduce some of the problems of insuring cyber risk.

36 The German Association of Insurers (GDV) is already working on non-binding cyber policies templates (see http://www.gdv.de/2015/06/mehr-schutz-gegen-hacker/).

4. Derivation of Potential Future Work (Practical Perspective)

Based on these results of the Section 3, we now discuss potential areas of future work both from a practical as well as from an academic perspective. First, we consider what the insurance industry and what the government might do to prevent cyber risk and to support cyber insurance. We focus the discussion on the role of the insurance industry and government, but also acknowledge the important role of other fields (e.g. IT security) in developing the topic of cyber risk and cyber insurance. These aspects are partly discussed in some places, but are not the main focus of the paper.

Table 6 provides an overview of international initiatives on cyber risk and cyber insurance and illustrates that many supranational organisations both from the industry as well as on the governmental side are now actively developing cyber risk as part of their strategic agenda[37]. The discussion in the next two subsections reflects both the results from Section 3 as well as the discussions within these international initiatives. As such, many of the recommendations are already actively implemented.

Table 6: Overview on international initiatives on cyber risk and cyber insurance

Institution	Contribution
International Association of Insurance Supervisors (IAIS)	Issues Paper on Cyber Risk to the Insurance Sector
Global Federation of Insurance Associations (GFIA)	GFIA Ad Hoc Working Group on Cyber
Organisation for Economic Co-operation and Development (OECD)	OECD project on cyber risk insurance; Working Group for Privacy & Security in Single digital market
Chief Risk Officer (CRO) Forum	Cyber resilience—The cyber risk challenge and the role of insurance (CRO Forum, 2014); Concept Paper on a proposed categorisation methodology for cyber risk (CRO Forum, 2016)
The Geneva Association (GA)	Cyber Stocktaking Initiative
Federal Financial Institutions Examination Council (FFIEC)	Cybersecurity Assessment Tool
Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO, 2015)	Guidance on Cyber Resilience for Financial Market Infrastructures
World Economic Forum (WEF)	Global Risk Report
European Union Agency for Network and Information Security (ENISA)	Evaluation framework for Cyber Security Strategies
International Risk Governance Council (IRGC)	Task Force on Cyber Risk
Cambridge Centre of Risk Studies (2016)	Data scheme for the identification, quantification, and reporting of cyber risk
Office of Compliance Inspections and Examinations (OCIE)	OCIE's 2015 Cybersecurity Examination Initiative
European Commission (2016)	Cooperation, information exchange, education, and establishment of public–private partnership
Singapore's Nanyang Technological University (NTU) and partners (Asia Insurance Review, 2016)	Cyber Risk Management (CyRiM) Project: aims to improve protection of the public, private and household sectors against cyber-attacks.

37 Table 6 is limited to international initiatives; not listed are the manifold national initiatives both in the private and public sector, e.g. by the Homeland of Security in the U.S., the Association of British Insurers (ABI) in the U.K. or the Monetary Authority of Singapore (MAS).

4.1. What should the insurance industry do to prevent cyber risks and to support cyber insurance?

- The insurance industry should work together globally with other stakeholders in order to develop standards, common language, and good practices.
- The industry should establish anonymised data pools and develop (re-)insurance pools.
- Insurers should conduct scenario analysis, track technological development (cloud computing, Internet of Things, block chain technology etc.), improve own analytical skills, make own IT more resilient, revise existing policies and develop new ones.

One of the current problems in the management of cyber risk is the lack of standards, a common vocabulary and best practices. The insurance industry should globally work together with other stakeholder to collecting and spreading such information. One first idea would be to publish methods (standards and good practices) for cyber risk assessment. An element, for example, could be to provide a common scheme to classify cyber-related loss events (see AIR Worldwide, 2016 and Risk Management Solutions, 2016). Besides the management of 'daily life' cyber risks, extreme scenarios seem to be of special concern. Here the insurance industry should further intensify the analysis of extreme loss scenarios in order to get a better sense of the loss severities and frequencies. Risk management approaches for complex crises, that is, methodologies, models or tools for mastering complexity are needed. Such approaches are useful not only for the insurance industry itself, but also for their clients (i.e. other industries) and society as a whole. In this context, one important activity could also be for the insurance industry to initiate or further intensify the dialogue on cyber risk with the relevant stakeholders. One important stakeholder, for instance, could be the government. The insurance industry should support the government in the preparation of national cyber risk strategies.

Another aspect on the technical side is the continuous tracking of technological developments. This is especially important given that new technologies might accelerate cyber risk. One example is cloud computing and the question of how to protect the cloud. The integrity and confidentiality of outsourced data can be highly questioned. Moreover, as the Internet of Things develops, another technical question is how to prevent attacks on autonomous systems like smart grids (both in private households as well as in industry). The Internet of Things will increase the vulnerability of operational technology (OT) as discussed in Section 3.1. Another example is block chain technology, e.g. in the context of bitcoin technology, which is increasingly being used by Fintechs, but also by traditional banks. In general, it seems that there is high dependence on a few platform providers (e.g. cloud service providers like Amazon, Google, and Microsoft) and software firms (like Microsoft, Oracle, SAP etc.). The failure of one of these will impact millions of people and organisations simultaneously. From a risk management point of view, one important question is thus what architectural improvements of a company's IT system might increase resilience to cyber risk.[38]

Regarding cyber insurance, an anonymised data pool might be the easiest way to intervene in the insurance market. Common knowledge can be easily collected, standards could be more easily established, and—most importantly—data can be collected. The implementation will thus reduce uncertainties with respect to data and with respect to modelling. An anonymous data pool could be developed as a public–private partnership, that is, the industry can self-create and manage the pool. However, before setting up the data pool, the government has to set the legal framework, especially regarding competition law, since combining data might breach existing laws. First types of such pools already begin to exist in the U.S. in the context of cyber liability insurance, although the samples are relatively small (e.g. NetDiligence, 2015, reports 160 data breach insurance claims).

38 There are manifold other points that might be included in the discussion on new technologies. Among these are the use of big data and digital forensics, i.e. the further automation of forensic methods, the ability to analyse and correlate large data sources and also the forensic analysis of novel technologies (cloud, IoT etc.).

The implementation of a data pool might be connected with the creation of an insurance pool (e.g. LongFinance, 2015; Eling and Wirfs, 2016b). This approach could resolve the problems related with relatively small insurance portfolios and diversification issues. One major advantage of such an insurance pool is the opportunity to accumulate risks of the same type in one portfolio and thereby guarantee the critical size needed to benefit from diversification effects. Essential to achieve those benefits is the introduction of a fair sharing mechanism among the pool members (e.g. Fragnelli and Marina, 2003; Ambrosino *et al*., 2006; or Kraut, 2014). Furthermore, in insurance pools, the insurance market's resources, for instance capital, knowledge and experience, can be bundled and allow the underwriting of heavy risks, something that the single pool member would not be able to do (e.g. Reichel and Schmeiser, 2015). Aside from risk sharing, the main advantage of a pool is the sharing of data and expertise in order to better understand and calculate risks. The creation of a pool for cyber risk has already been discussed for the U.K. in the context of a reinsurance pool (Long Finance, 2015). According to Long Finance (2015), three factors make the pooling of cyber risks necessary: (1) the insurance industry lacks the capacity to cover a catastrophic cyber event; (2) existing cyber coverage will only cover a small portion of losses (e.g. associated with data breaches, network disruption), leaving a significant portion of risks in the economy uninsured; and (3) the U.K. government is not yet able to back up potentially unlimited liabilities in the event of a catastrophic cyber event that could threaten the whole country's economy. Hence, they suggest a public–private partnership, where the insurer's retention levels and the pool's funds must be exhausted before the state enters the risk transfer as a reinsurer of last resort. The U.K. has already adopted such schemes for other risk categories (e.g. Pool Re for terrorism and Flood Re for natural catastrophes; see Long Finance, 2015). Alternatively, the insurance industry could also increase the underwriting capacity by defining different layers and splitting the claims between several primary and reinsurers.

However, from an economic point of view, the introduction of an insurance pool constitutes a severe intervention into the free markets that can be justified only with the presence of severe market failures in the absence of intervention. A lack of insurability is an example of the kind of market failure that might justify an intervention. It remains, however, an empirical question whether the existing risk capacity is so small that a strict intervention like pooling can be justified. Some market participants rather argue that the existing risk capacity is already sufficiently high so that a pooling to increase capacity is not really needed.

Finally, the insurance industry should work together with other stakeholders to raise awareness of cyber risk and educate clients on how to deal with it. It could define risk management practices that clients need to comply with in order to buy cyber policies. The industry could even provide clients with tools helping them to protect against cyber risks as has been done for other lines of business. Moreover, it is also important that insurers build up the required IT security knowledge or tap the competence of specialised firms. Sales and risk management need to acquire specific technical IT knowledge in order to understand cyber risk sufficiently. It might even be advisable to hire people with an IT background for such positions. Moreover, the distribution channels (brokers) might need to be reviewed and adapted to the specific challenges cyber insurance poses. For example, some brokers are actively developing their own policies and asking the markets to accept them. The dynamic nature of cyber risk may prove this to be an undesirable practice. Brokers are not evaluating the risk from an aggregation perspective within the cyber market or across commercial insurance products. Biener, Eling, Matt and Wirfs (2015) mention that the lack of understanding, both on the demand and supply side, is one of the main limitations of the cyber insurance market.

4.2. What should the government do to prevent cyber risks and to support cyber insurance?

- To prevent cyber risks: tackle cybercrime by international collaboration, initiate global dialogues and conventions aimed at confining cyberwars, boost IT landscape resilience, support development of cyber databases, introduce reporting requirements and minimum standards for risk mitigation.

- To support cyber insurance: consider public–private partnerships with the government as insurer of last resort (governmental backstop for extreme scenarios); incentivise the development of an anonymised data pool; facilitate the development of traditional and alternative risk transfer mechanisms.

As a major share of cyber risk losses is caused by **cyber criminality**, governments could reduce cyber risk threats by imposing more severe **punishments** and increasing the resources for law enforcement. As the technological environment is continuously changing and the attacks get more sophisticated, it is especially important that investigative authorities are equipped with sufficient resources in order to keep up. However, as cyber criminality is not restricted by national boundaries, purely national legal frameworks are likely to remain rather ineffective. To some extent it is the country with the weakest legal system and the highest cyber criminality that determines the global cyber threat level. Therefore, **international collaboration**, such as some minimal **criminal law** standards, the exchange of information and interstate rendition, is urgently needed.

Governments also need to be prepared for acts of **cyberwar**. Many countries' answer to this emerging threat has been to build up their own cyberwar teams, be it as a means of passive or even active **defence**. It is estimated that more than 100 countries maintain special cyberwar forces (NZZ, 2014). This shows that some kind of **digital arms race** is already under way that might be rational from each country's perspective but, globally, it is a waste of resources and causes welfare losses. Countries might even use conventional warfare as a response to cyberwar attacks. This development is also reflected in the Tallinn Manual on the International Law Applicable to Cyber Warfare (Schmitt, 2013), which tends to lowers the hurdles for cyber-attacks being classified as an act of war. As such, not only the use of preventive military strikes would be legitimated, but also excessively collection of data, surveillance and espionage. Instead of these responses, we think **international dialogues** aimed at **cyber disarmament** and **conventions** and **codices** in order to restrict the use of cyber weapons as has been done for weapons of mass destruction should be promoted.

As cyber losses are frequently caused by vulnerabilities of or failures in **soft- or hardware** components, regulation could also be directly aimed at technology firms. Expanding the **product liability** for IT products would be one way to improve their quality and safety. Another approach could be to require minimal **standards for the testing procedure** before the product's roll-out.[39] However, as illustrated in this paper, the problem might not only be faulty products but that only a very few products are widely applied. This homogeneous IT landscape might allow risk to spread and cause systemic risk. Increasing diversity of IT solutions could be a way to increase overall resilience (see Böhme, 2005). **Competition laws and authorities** should include these considerations in their decision-making.

Governments might introduce **reporting obligations** to prevent cyber risk and to promote the development of the cyber insurance market. The reporting obligations could eventually be enforced with **penalties**. Every manager gets the incentive to do the best to prevent cyber risk, because in the event of a cyber-attack significant market discipline from investors, analysts and customers can be expected. Reporting obligations in the European Union already passed legislation, and we believe other countries should also discuss the introduction. It remains an empirical question whether reporting obligations might cause the same trigger effect as in the U.S. cyber insurance market (considering differences in legal systems, risk culture etc. when comparing Europe and the U.S.), but we believe that it is more likely to foster the development of the insurance market.

39 Peiter Zatko (Mudge) proposed a testing procedure for software that can be used to produce a security rating (The Intercept, 2016).

In a similar direction, governmental institutions could support the establishment of **cyber risk databases**. An example is the National Vulnerability Database (NIST) in the U.S. that collects reported software vulnerabilities. Similar repositories could be built for malware or security breaches. A central institution would be able to provide quickly relevant information on new developments so that people responsible for IT risk management can act in time. As mentioned above, people might not be fully aware of the threat of cyber risk. Therefore, governments should conduct campaigns in order to improve education and raise awareness. For example, the Swiss intelligence service is currently running a campaign in order to increase the awareness of high tech companies and research institutes with regard to cyber espionage.

Another measure could be the definition of minimal standards for **risk mitigation**. Minimal standards for risk mitigation will reduce incentives for moral hazard, which is one of the main insurability challenges of cyber risk. Furthermore, it might help to provide a minimal level of security, which then reduces contagion, and in doing so, mitigates problems with dependence of losses. A regulatory intervention like this could be justified on economic grounds, given that cyber security is a public good with positive externalities.

The government also has an interest in improving the **insurability of cyber risks** in order to protect the economy from harmful scenarios that could endanger economic well-being. The subsidisation of traditional risk transfer mechanisms could also be interesting for a governmental intervention measure. Without intervening directly, the government might provide incentives for private risk transfer mechanisms. One example could be to support the private insurance industry with the implementation of an **insurance pool**. The government could motivate the industry to set up an insurance pool for a limited time period or for selected aspects of cyber risk, such as extreme scenarios. Furthermore, the state could incentivise the introduction of **capital market solutions** by emitting cyber cat bonds for selected risks.[40] Again, we emphasise that we do not postulate that all the measures need or can be implemented, but they might be fruitful directions for discussions between the stakeholders to improve the insurability of cyber risks.

40 Although a cyber cat bond seems to be a construct for the future, recently there are first discussions and transactions that are also related to cyber. See several articles on www.artemis.bm or the recent Credit Suisse operational risk cat bond.

5. Derivation of Potential Future Research (Academic Perspective)

- Micro perspective: conduct more research on the demand side (e.g. risk perception, fatalism), analyse insurability and ways to improve insurability (especially empirical research, e.g. data generation, data and scenario analysis), analyse optimal risk management (mitigation vs insurance) and how much capital is needed to cover cyber risks, collaborate more with other stakeholders globally.

- Macro perspective: conduct more scenarios analyses for measurement and management of accumulation risk, analyse the systemic risk potentially emerging from cyber risk underwriting, become part of the global dialogue with stakeholders.

Regarding future research, one aspect to note is that the existing research in the risk and insurance domain mainly focuses on the supply side aspects of insurability. The demand side, however, has not yet been subject of much research. More could be done, e.g. analysing the risk perception of customers both in commercial and in retail business. One interesting behavioural element in this context is the latent fatalism many people show with respect to cyber risk ('it will not happen to me'; 'my data are not interesting enough'). Identifying the underlying drivers of this perception and increasing awareness might help to increase the demand for cyber risk insurance. It might also be interesting to compare risk perception and risk aversion in the field of cyber risk insurance with other types of insurances or other types of risks (e.g. from the capital market).

In general, more empirical research is needed, both on the demand and the supply sides. What risk characteristics (e.g. correlation) determine whether insurance or self-protection is economically more efficient risk management tool for cyber risk? What capital standards are needed for cyber risk, both for own cyber risk and for underwriting cyber risk? Also, the link between new technologies and insurance will give rise to research questions. For example, what should liability insurance look like in the context of self-driving cars or in the context of the Internet of Things? How will the economy and society change in light of ongoing globalisation and digitalisation? More specifically, what does it mean for the insurance idea to provide solidarity and a community of good and bad risks? What if, for example, the true risk profile is fully known to the insurance company and the policyholder (as in pay-as-you-drive or pay-as-you-live concepts)?

Regarding the macro perspective, more scenarios for measurement and management of accumulation risk are needed. Another question related to the macro perspective is whether the sales of cyber insurance could create a risk between different companies. As cyber risk tend to be globally correlated, the underwriting sides of different insurers tend to be affected simultaneously. Finally, also the academic community should be part of the global dialogue on how to prevent cyber risk and how to promote cyber insurance in order to provide their point of view in the discussions.

References

Ablon, L., Libicki, M. C. and Golay, A. A. (2014) *Markets for cybercrime tools and stolen data: hackers bazaar*, Santa Monica, CA: Rand Corporation.

Advisen (2015) Cyber risk insights conference, 10 February 2015, London, http://www.advisenltd.com/wp-content/uploads/london-cyber-risk-insights-conference-slides-2015-02-17.pdf, last accessed 4 May 2016.

Ahamad, M. (2012) What if a hacker caused a large-scale internet outage?, https://www.weforum.org/agenda/2012/06/what-if-a-hacker-caused-a-large-scale-internet-outage/, last accessed 4 May 2016.

AIR Worldwide (2016) *Verisk cyber exposure data standard and preparer's guide*, http://www.air-worldwide.com/Documentation/Cyber-Exposure-Data-Standard/Index.htm, last accessed 2 June 2016.

Allianz (2011) How long can a company survive without a functioning IT system?, https://www.allianz.com/en/press/news/company/point_of_view/news_2011-09-27.html/, last accessed 29 June 2016.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M.J.G., Levi, M., Moore, T. and Savage, S. (2013) 'Measuring the cost of cybercrime', in R. Böhme (ed.), *The Economics of Information Security and Privacy*, Heidelberg: Springer, pp. 265–300.

Ambrosino, D., Fragnelli, V. and Marina, M. . (2006) 'Resolving an insurance allocation problem: A procedural approach', *Social Choice and Welfare* 26(3): 625–643.

Asia Insurance Review (2016) 'NTU partners re/insurers to launch cyber risk management initiative', http://www.asiainsurancereview.com/News/View-NewsLetter-Article?id=35924&Type=eDaily, last accessed 29 October 2016.

Australian Signals Directorate (ASD) (2014) *Strategies to mitigate targeted cyber intrusions*, http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf, last accessed 29 June 2016.

Bank for International Settlements (BIS) (2006) *International convergence of capital measurement and capital standards: A revised framework comprehensive version*, Basel: BIS www.bis.org/publ/bcbs128.pdf, last accessed 10 December 2013.

Bashan, A., Berezin, Y., Buldyrev, S.V. and Havlin, S. (2013) 'The extreme vulnerability of interdependent spatially embedded networks', *Nature Physics* 9(10): 667–672.

Beckstrom, R. (2012) 'What if a hacker caused a large-scale Internet outage?', https://www.weforum.org/agenda/2012/06/what-if-a-hacker-caused-a-large-scale-internet-outage, last accessed 5 May 2016.

Berliner, B. (1982) *Limits of Insurability of Risks*, Englewood Cliffs, NJ: Prentice-Hall.

Betterley (2013) *The Betterley report—cyber/privacy insurance market survey* 2013, http://betterley.com/samples/cpims13_nt.pdf, last accessed 4 May 2016.

Betterley (2015) *The Betterley report—cyber/privacy insurance market survey* 2015, http://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf, last accessed 4 May 2016.

Biener, C., Eling, M. and Wirfs, J.H. (2015) 'Insurability of cyber risk: an empirical analysis', *The Geneva Papers on Risk and Insurance—Issues and Practice* 40(1): 131–158.

Biener, C., Eling, M., Matt, A. and Wirfs, J.H. (2015) *Cyber Risk: Risikomanagement und Versicherbarkeit*, I.VW-Schriftenreihe, Band 54, St. Gallen: Institute of Insurance Economics I.VW-HSG.

Böhme, R. and Kataria, G. (2006) *Models and measures for correlation in cyber-insurance*, working paper presented at the Fifth Workshop on the Economics of Information Security (WEIS), 26–28 June 2006, University of Cambridge, U.K.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2008) *BSI-Standard 100-2: IT-Grundschutz: Vorgehensweise*, Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile&v=1, last accessed 28 June 2016.

Cambridge Centre of Risk Studies (CCRS) (2016) *Cyber insurance exposure data schema v1.0*, Cambridge Risk Framework series, http://cambridgeriskframework.com/getdocument/38, last accessed 19 May 2016.

Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003) 'The economic cost of publicly announced information security breaches: empirical evidence from the stock market', *Journal of Computer Security* 11(3): 431–448.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004) 'The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers', *International Journal of Electronic Commerce* 9(1): 70–104.

Chavez-Demoulin, V., Embrechts, P. and Nešlehová, J. (2006) 'Quantitative models for operational risk: extremes, dependence and aggregation', *Journal of Banking & Finance* 30(10): 2635–2658.

Cebula, J.J. and Young, L.R. (2010) *A taxonomy of operational cyber Security risks*, Technical Note CMU/SEI-2010-TN-028, Pittsburgh, PA: Carnegie Mellon University.

Clarke, R.A. and Knake, R.K. (2015) 'Cyber war: the next threat to national security and what to do about it?', *Strategic Analysis* 39(4): 458–460.

Center for Internet Security (CIS) (2016) *The CIS critical security controls for Effective Cyber Defense: Version 6.0*, https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf, last accessed 19 May 2016.

CRO Forum (2014) *Cyber resilience—the cyber risk challenge and the role of insurance*, http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance, last accessed 5 May 2016.

CRO Forum (2016) CRO *Forum concept paper on a proposed categorisation methodology for cyber risk*, http://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web.pdf

De Montjoye, Y.A., Radaelli, L., Singh, V.K. and Pentland, A. (2015) 'Unique in the shopping mall: on the reidentifiability of credit card metadata', *Science* 347(6221): 536–539.

Department for Business, Innovation & Skills and Cabinet Office (2014) *Cyber essentials scheme: summary*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf, last accessed 5 May 2016.

Edwards, B., Hofmeyr, S. and Forrest, S. (2015) 'Hype and heavy tails: a closer look at data breaches', working paper presented at the 14th Annual Workshop of the Economics of Information Security, 22–23 June 2015 Delft, The Netherlands.

Eling, M. and Wirfs, J. H. (2016a) *Cyber risk: too big to insure? Risk transfer options for a mercurial risk class*, I·VW HSG Schriftenreihe, Band 59, St. Gallen: Institute of Insurance Economics I.VW-HSG, http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf, last accessed 6 May 2016.

Eling, M. and Wirfs, J. H. (2016b) *Modelling and management of cyber risk*, working paper.

European Commission (2016) Commission boosts cybersecurity industry and steps up efforts to tackle cyber-threats, http://europa.eu/rapid/press-release_MEMO-16-2322_en.htm.

Finkle, J. (2015) Ace offers $100 million cyber policies with added services, scrutiny, http://www.reuters.com/article/us-ace-ltd-cyberinsurance-idUSKCN0RO2LD20150924, last accessed 5 November 2015.

Fitch Ratings (2016) Rapid growth in cyber insurance would be credit-negative, https://www.fitchratings.com/site/pressrelease?id=1001233, last accessed 2 June 2016.

Fragnelli, V. and Marina, M.E. (2003) 'A fair procedure in insurance', *Insurance: Mathematics and Economics* 33(1): 75–85.

Geschonnek, A., Fritsche, T. and Weiand, K. (2013) *E-Crime—Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz*, KPMG Forensic Services, https://www.tns-emnid.com/studien/pdf/studie_e-crime.pdf, last accessed 18 January 2014.

Gordon, L.A., Loeb, M.P. and Sohail, T. (2003) 'A framework for using insurance for cyber-risk management', *Communications of the* ACM 46(3): 81–85.

Harvard Business Review Analytic Services (2013) *Meeting the cyber risk challenge*, Boston, MA: Harvard Business School Publishing, http://www.ferma.eu/app/uploads/2013/01/Cyber-risks-report1.pdf.

Helbing, D. (2013) 'Globally networked risks and how to respond', *Nature* 497(7447): 51-59.

Herath, H. and Herath, T. (2011): 'Copula-based actuarial model for pricing cyber-insurance policies', *Insurance Markets and Companies: Analyses and Actuarial Computations* 2(1), 7–20.

Hochstätter, C.H. and Masiero, M. (2009): *Angriffe auf das Internet: Wie realistisch ist der Totalausfall?*, White Paper, http://www.zdnet.de/41005661/angriffe-auf-das-internet-wie-realistisch-ist-der-totalausfall, last accessed 5 May 2016.

Hofmann, A. and Ramaj, H. (2011): Interdependent risk networks: the threat of cyber attack, *International Journal of Management and Decision Making* 11(5/6): 312–323.

Hovav, A. and D'Arcy, J. (2003) 'The impact of denial-of-service attack announcements on the market value of firms', *Risk Management and Insurance Review* 6(2): 97–121.

Hua, J. and Bapna, S. (2013) 'The economic impact of cyber terrorism', *The Journal of Strategic Information Systems* 22(2): 175-186.

Kaspersky Lab (2013) *Global corporate IT security risks*: 2013, www.kasperskycontenthub.com/presscenter/files/2013/10/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf, last accessed 24 April 2014.

Kelly, S., Leverett, E., Oughton, E.J., Copic, J., Thacker, S., Pant, R.,… Hall, J.W. (2016) *Integrated Infrastructure: Cyber resiliency in society: mapping the consequences of an interconnected digital economy*, Cambridge Risk Framework series, Cambridge: Centre for Risk Studies, University of Cambridge.

Kraut, G. (2014) *A fair pool sharing mechanism for illiquid catastrophe risk markets*, Munich Risk and Insurance Center Working Paper No. 19.

Krieger, F. (2015) 'S&P: US-Versicherer haben Cybersparte im Griff', *Herbert Frommes Versicherungsmonitor*, http://versicherungsmonitor.de/2015/06/sp-us-versicherer-haben-cybersparte-im-griff, last accessed 28 June 2016.

Kshetri, N. (2010) *The Global Cybercrime Industry*, Berlin/Heidelberg: Springer.

Lloyd's (2015a) A quick guide to cyber risk, https://www.lloyds.com/news-and-insight/news-and-features/emerging-risk/emerging-risk-2015/a-quick-guide-to-cyber-risk, last accessed 5 May 2016.

Lloyd's (2015b) *Business blackout—the insurance implications of a cyber attack on the US power grid*, https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf, last accessed 6 November 2015.

Long Finance (2015) 'Promoting UK cyber prosperity: public-private cyber-catastrophe reinsurance', http://www.longfinance.net/images/Promoting_UK_Cyber_Prosperity_28 July 2015.pdf, last accessed 16 September 2015.

National Association of Insurance Commissioners (NAIC) (2013) Cybersecurity, http://www.naic.org/cipr_topics/topic_cyber_risk.htm, last accessed 4 May 2016.

National Conference of State Legislatures (NCSL) (2016) Security breach notification laws, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, last accessed 4 May 2016.

National Institute of Standards and Technology (NIST) (2016) National vulnerability Database, https://web.nvd.nist.gov/view/vuln/search-results?query=&search_type=all&cves=on, last accessed 5 May 2016.

NetDiligence (2014) *Cyber claims study 2014*, http://www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf, last accessed 5 May 2016.

NetDiligence (2015) *Cyber claims study 2015 -*, http://www.netdiligence.com/downloads/NetDiligence_2015_Cyber_Claims_Study_093015.pdf, last accessed 5 May 2016.

New York state department of financial services (2016) Cybersecurity requirements for financial services companies', http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf, last accessed 29 Oktober 2016.

Maillart, T. and Sornette, D. (2010) 'Heavy-tailed distribution of cyber-risks', *The European Physical Journal* B 75(3): 357-364.

Marsh (2012) 'Cyber insurance', www.iod.org.nz/Portals/0/Branches%20and%20events/Canterbury/Marsh%20Cyber%20Insurance.pdf, last accessed 17 January 2014.

Marsh (2013) 'Cyber risk survey 2013', https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20Survey%2006-2013.pdf, last accessed 19 September 2016.

McAfee (2014) *Net losses: estimating the global cost of cybercrime*, http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf, last accessed 16 March 2015.

Moody's (2015) Threat of cyber risk is of growing importance to credit analysis, https://www.moodys.com/research/Moodys-Threat-of-cyber-risk-is-of-growing-importance-to--PR_339656, last accessed 2 June 2016.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukan, S.K. (2013) 'Cyber-risk decision models: to insure it or not?', *Decision Support Systems* 56(1): 11–26.

Mukhopadhyay, A., Saha, D., Mahanti, A., Chakrabarti, B.B. and Podder, A. (2005) 'Insurance for cyber-risk: a utility model', *Decision* 32(1): 153–169.

Office of Compliance Inspections and Examinations (OCIE) (2015) 'OCIE's 2015 cybersecurity examination initiative', National Exam Program Risk Alert 4(8): 1–8, https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf, last accessed 2 June 2016.

Office of the Superintendent of Financial Institutions (2013) Cyber security self-assessment guidance, http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx, last accessed 10 June 2016.

Ögüt, H., Raghunathan, S. and Menon, N. (2011) 'Cyber security risk management: public policy implications of correlated risk: imperfect ability to prove loss, and observability of self-protection', *Risk Analysis* 31(3): 497–512.

Ponemon Institute (2013) *Managing cyber security as a business risk: cyber insurance in the digital age*, http://www.ponemon.org/blog/managing-cyber-security-as-a-business-risk-cyber-insurance-in-the-digital-age, last accessed 18 January 2014.

Ponemon Institute (2015a) *2015 cost of cyber crime study: global*, http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report, last accessed 3 March 2016.

Ponemon Institute (2015b) *2015 cost of data breach study: global analysis*, https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF, last accessed 3 March 2016.

Rakes, T.R., Deane, J.K. and Rees, L.P. (2012) 'IT security planning under uncertainty for high-impact events', *Omega* 40(1): 79–88.

Refsdal, A., Solhaug, B. and Stølen, K. (2015) *Cyber-Risk Management*, Cham: Springer International Publishing.

Reichel, L. and Schmeiser, H. (2015) *The liability regime of insurance pools and its impact on pricing*, Institut für Versicherungswirtschaft Working Paper No. 168, St. Gallen: Institute of Insurance Economics, University of St. Gallen.

Risk Management Solutions, Inc. (RMS) (2016) *Managing cyber insurance accumulation risk*, Centre for Risk Studies, University of Cambridge.

Ruffle, S.J., Bowman, G., Caccioli, F., Coburn, A.W., Kelly, S., Leslie, B. and Ralph, D. (2014) *Stress test scenario: sybil logic bomb cyber catastrophe*, Cambridge Risk Framework series, Centre for Risk Studies, University of Cambridge.

Schmitt, M. N. (ed.) (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge/New York: Cambridge University Press.

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

Sinanaj, G. and Muntermann, J. (2013) 'Assessing corporate reputational damage of data breaches: an empirical analysis', *Proceedings of the 26th International Bled eConference*, pp. 78-89.

Standard & Poor's (2015) *Cyber risk and corporate credit*, http://www.maalot.co.il/publications/OAC20150708094842.pdf, last accessed 2 June, 2016.

Strickland, J. (2010) What would happen if the internet collased?, http://computer.howstuffworks.com/internet/basics/internet-collapse.htm, last accessed 5 May 2016.

Swiss Re (2014) 'Working together with clients to find cyber risk solutions', http://www.swissre.com/reinsurance/insurers/casualty/smarter_together/Working_smarter_together_for_cyberrisk_solutions.html, last accessed 18 March 2015.

Symantec Corporation (2013) 2013 Norton report, http://www.symantec.com/content/de/de/about/downloads/2013_Norton_Report_Deck.pdf, last accessed 16 March 2015.

Symantec Corporation (2015) *Internet security threat report*—April 2015, https://www.symantec.com/security-center/threat-report, last accessed 4 May 2016.

Symantec Corporation (2016) ', https://www.symantec.com/security-center/threat-report, last accessed 4 May 2016.

The Intercept (2016) *A Famed Hacker Is Grading Thousands of Programs — and May Revolutionize Software in the Process*, https://theintercept.com/2016/07/29/a-famed-hacker-is-grading-thousands-of-programs-and-may-revolutionize-software-in-the-process, last accessed 30 October 2016.

TeleGeography (2016) Submarine cable map, http://www.submarinecablemap.com/, last accessed 18 November 2016.

U.S. Securities and Exchange Commission (SEC) (2016) *CF Disclosure Guidance: Topic No. 2*, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm, last accessed 28 October 2016.

VdS Schadenverhütung GmbH (2015) *Cyber security for small and medium enterprises (SMEs)*, brochure', https://vds.de/fileadmin/vds_publikationen/vds_5555en_web.pdf, last accessed 28 June 2016.

Verizon (2016) *'2016 data breach investigations report: 89% of breaches had a financial or espionage motive*, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf, last accessed 2 June 2016.

Wheatley, S., Maillart, T. and Sornette, D. (2015) *The extreme risk of personal data breaches & the erosion of privacy*, working paper, Cornell University Library, http://arxiv.org/abs/1505.07684, last accessed 17 November 2015.

Willis (2013a) Insurance—cyber risk, http://www.pwc.dk/da/arrangementer/assets/cyber-tineolsen.pdf, last accessed 5 May 2016.

Willis (2013b) *Willis Fortune 1000 cyber disclosure report*, http://blog.willis.com/wp-content/uploads/2013/08/Willis-Fortune-1000-Cyber-Report_09-13.pdf, last accessed 4 May 2016.

World Economic Forum (WEF) (2010) *Global risk report 2010—a global risk network report*, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2010.pdf, last accessed 17 November 2015.

World Economic Forum (WEF) (2014) *Global risks 2014—ninth edition*, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf, last accessed 17 June 2016.

World Economic Forum (WEF) (2015) *Global risks report 2015—tenth edition*, http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf, last accessed 9 October 2015.

YouGov (2014) Cyber Risiken im Privatbereich, https://yougov.de/loesungen/reports/studien/cyberrisiken, last accessed 14 June 2016.

Zürich (2015) *Risk nexus: overcome by cyber risks? Economic benefits and costs of alternate cyber futures*, http://publications.atlanticcouncil.org/cyberrisks, last accessed 29 June 2016.

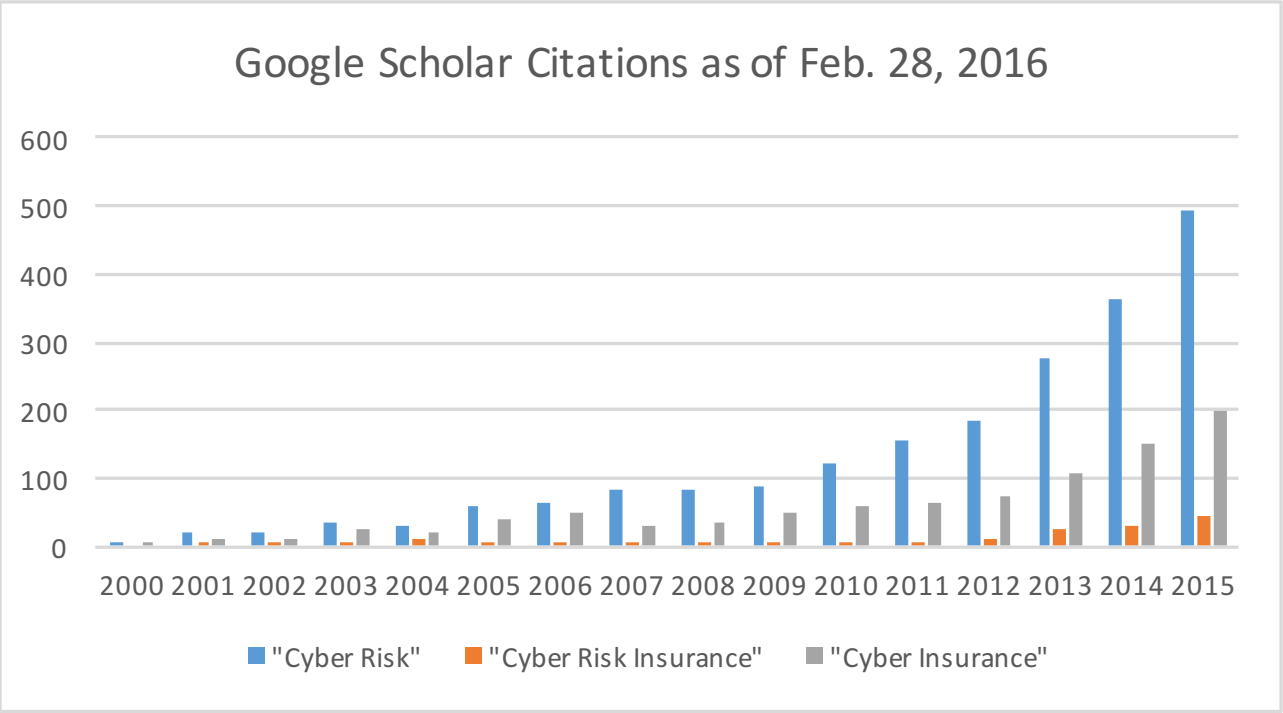
Appendices

Appendix A: Increasing relevance of cyber risk and cyber risk insurance

Table A1: Google Scholar citations as of 28 February 2016

Year	'Cyber Risk'	'Cyber Risk Insurance'	'Cyber Insurance'
2000	7	0	6
2001	19	4	12
2002	19	3	10
2003	35	6	24
2004	31	10	21
2005	59	7	39
2006	63	8	51
2007	83	8	28
2008	82	6	33
2009	88	5	52
2010	120	4	57
2011	157	5	64
2012	187	11	76
2013	275	27	106
2014	364	29	152
2015	494	44	199

Figure A1: Google Scholar citations as of 28 February 2016



Note: Papers that contain the words 'cyber risk' or 'cyber insurance' do not necessarily discuss this topic as main field, but also might cover it as a side aspect.

Appendix B: Search and Identification Strategy

- We search for the terms 'cyber risk', 'cyber risk insurance' and 'cyber insurance' in the journal databases EBSCOhost (Business Source Premier and EconLit) and ABI/INFORM Complete. In addition, we searched for the terms in the Social Science Research Network (SSRN) and via Google Scholar.

- We review journal issues from January 2000 to December 2015 of the following journals: Journal of Finance, American Economic Review, Journal of Risk and Insurance, Insurance: Mathematics and Economics, The Geneva Papers on Risk and Insurance—Issues and Practice, and The Geneva Risk and Insurance Review. Other journals from the field of risk and insurance are also reviewed (Journal of Insurance Regulation, Risk Management & Insurance Review, ASTIN Bulletin, North American Actuarial Journal, European Actuarial Journal).

- We review all working papers from the annual meetings of the American Risk and Insurance Association (ARIA) for 2011, 2012, and 2013, the 2010 and 2015 World Risk and Insurance Congress, and other relevant conferences in the fields (EGRIE, APRIA).

- We reviewed citations in relevant studies to identify additional relevant material.

The search and identification strategy described here has been used in various projects and articles (see e.g. www.casact.org/rpp2).

Appendix C: List of Cyber Risk Literature

ID	Title	Author(s)	Year	Journal	Volume	Issue/ No.	Pages	
1	If most of your revenue is from e-commerce, then cyber-insurance makes sense	Luzwick, P.	2001	Comput. Fraud. Secur.	3		16-17	
2	Convention on cybercrime	Council of Europe	2001	online				
3	Cyber-risk management: technical and insurance controls for enterprise-level security	Siegel, C.A., Sagalow, T.R., Serritella, P.	2002	Information Systems Security—Security Management Practices				
4	Risk management guide for information technology systems	Stoneburner, G., Goguen, A., Feringa, A.	2002	National Institute of Standards and Technology. Special Publication	800	30		
5	A framework for using insurance for cyber-risk management	Gordon, L. A., Loeb, M. P. and Sohail, T.	2003	Communications of the ACM	44	9	70-75	
6	The economic cost of publicly announced information security breaches: empirical evidence from the stock market	Campbell, K., Gordon, L.A., Loeb, M.P., Zhou, L.	2003	J. Comput. Secur.	11	3	431–448	
7	The impact of denial-of-service attack announcements on the market value of firms	Hovay, A. and D'Arcy, J.	2003	Risk. Manage.Insur. Rev.	6	2	97-121	
8	Creation of a global culture of cybersecurity, Resolution 57/239 adopted by the General Assembly	United Nations (UN)	2003	online				
9	The impact of denial-of-service attack announcements on the market value of firms	Hovav, A., & D'Arcy, J.	2003	Risk Management and Insurance Review	6	2	97-121	
10	A model for evaluating IT security investments	Cavusoglu, H., Mishra, B., Raghunathan, S.	2004	Commun. ACM	47	7	87-92	
11	The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers	Cavusoglu, H., Mishra, B., Raghunathan, S.	2004	Int. J. Electron. Comm.	9	1	69–104	

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	http://www.sciencedirect.com/science/article/pii/S1361372301030160	Industry	Management	Qualitative	Risk Management (Mitigation / Insurance)		
	https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId	Industry	Law	Qualitative	Risk Management (broad sense)	Regulation	
	http://www.tandfonline.com/doi/abs/10.1201/1086/43322.11.4.20020901/38843.5	Academia	IT	Qualitative	Risk Management (Mitigation / Insurance)	IT Security	
	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf	Industry	IT				
	http://dl.acm.org/citation.cfm?id=636774	Academia	Management	Qualitative	Risk Management (Mitigation / Insurance)	Asymmetric Information, Cyber Insurance	
	http://iris.nyit.edu/~kkhoo/Spring2008/Topics/Topic10/EconCostPubliclyAnnouncedSecurityBreaches-EmpStockMrkt2003.pdf	Academia	Finance / Insurance / RM	Empirical	Risk Monitoring		
	http://onlinelibrary.wiley.com/doi/10.1046/J.1098-1616.2003.026.x/abstract	Academia	Management	Empirical	Risk Monitoring	Event Study	
	http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf	Industry	Economics	Qualitative	Risk Management (broad sense)	Regulation	
	http://onlinelibrary.wiley.com/doi/10.1046/J.1098-1616.2003.026.x/abstract	Academia	IT	Empirical	Risk Assessment		
	https://www.utdallas.edu/~huseyin/paper/investment.pdf	Academia	IT	Theoretical	Risk Management (Mitigation / Insurance)	IT Security	
	https://www.utdallas.edu/~huseyin/paper/market.pdf	Academia	Finance / Insurance / RM	Empirical	Risk Monitoring	IT Security, Event Study	Capital markets, event study,

ID	Title	Author(s)	Year	Journal	Vol-ume	Issue/ No.	Pages	
12	Recognising and preparing loss estimates from cyber-attacks	Smith, G.S.	2004	Inf. Syst. Secur.	12	6	46–58	
13	Insurance for cyber-risk: a utility model	Mukhopadhyay, A., Saha, D., Mahanti, A. and Chakrabarti, B. B.	2005	Decision	32	1	153–169	
14	Cyber-insurance revisited	Böhme, R.	2005	Fourth Workshop on the Economics of Information				
15	The emerging cyber risks of biometrics	Barton, B., Byciuk, S., Harris, C., Schumack, D., & Webster, K	2005	Risk Management	52	1	26-28	
16	The effect of network topology on the spread of epidemics	Ganesh, A., Massoulié, L., & Towsley, D.	2005	In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE	2		1455-1466	
17	Models and measures for correlation in cyber-Insurance	Böhme, R. and Kataria, G.	2006	Working Paper, Workshop on the Economics of Information Security (WEIS) University of Cambridge, UK				
18	The evolution of cyberinsurance	Majuca, R. P., Yurcik, W., & Kesan, J. P.	2006					
19	Time-to-compromise model for cyber risk reduction estimation	McQueen, M. A., Boyer, W. F., Flynn, M. A., & Beitel, G. A.	2006	Springer US			49-64	
20	Quantitative cyber risk reduction estimation methodology for a small SCADA control system	McQueen, M. A., Boyer, W. F., Flynn, M. A., & Beitel, G. A.	2006	In System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on (Vol. 9, pp. 226-226). IEEE.	9		226-226	
21	E-risk management with insurance: a framework using copula aided Bayesian belief networks	Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Sadhukhan, S.K.	2006	39th Hawaii International Conference on System Sciences. Hawaii.				

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	http://www.tandfonline.com/doi/abs/10.1201/1086/44022.12.6.20040101/79786.8	Academia	Finance / Insurance / RM				
	https://www.researchgate.net/publication/236576735_Insurance_for_Cyber-risk_A_Utility_Model	Academia	Management	Theoretical	Risk Management (Mitigation / Insurance)	Cyber Insurance, Pricing, Risk Modelling	
	http://infosecon.net/workshop/slides/weis_5_1.pdf	Academia	Finance / Insurance / RM	Theoretical	Risk Assessment	Risk Modelling, Cyber Insurance	
	http://search.proquest.com/docview/227026083?pq-origsite=gscholar	Academia	Finance / Insurance / RM	Qualitative	Risk Identification	Data Breach	Biometrics, Risk management, Network security, Personal information, Privacy, Security management
	http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1498374&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1498374http://sec2013.crysys.hu/~mfelegyhazi/courses/EconSec/readings/09_BohmeK-2005insurance_correlation.pdf	Academia	IT	Theoretical	Risk Assessment		graph theory, hypercube networks internetworking, network servers routing protocols, security of data, table lookup telecommunication network topology telecommunication security
		Academia	Finance / Insurance / RM	Empirical	Risk Assessment	Risk Taxonomy, Risk Accumulation	
	https://arxiv.org/ftp/cs/papers/0601/0601020.pdf	Academia	Finance / Insurance / RM	Qualitative	Risk Assessment	Cyber Insurance, Insurability, Asymmetric Information	cyberinsurance, economics of information security
	http://www.if.uidaho.edu/~boyewf/docs/QoP_paper_2005.pdf	Academia	IT	Theoretical	Risk Management (Mitigation / Insurance)	Self Protection, IT security	
	http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1579754&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1579754	Academia	IT	Theoretical	Risk Management (Mitigation / Insurance)	Self Protection, IT security	Computer security Control systems Data security Hidden Markov models Laboratories
	https://www.computer.org/csdl/proceedings/hicss/2006/2507/06/250760126a.pdf	Academia	Finance / Insurance / RM	Theoretical	Risk Assessment	Risk Modelling, Interdependent Risks, Risk Accumulation	e-commerce, security breach, e-risk, Bayesian Belief Network (BBN), copula, premium

ID	Title	Author(s)	Year	Journal	Volume	Issue/ No.	Pages	
22	Cyberinsurance in IT security management	Baer, W. S., and Parkinson, A.	2007	IEEE Security and Privacy	5	3	50-56	
23	Cyber security risk assessment for SCADA and DCS networks	Ralston, P. A., Graham, J. H., & Hieb, J. L	2007	ISA transactions	46	4	583-594	
24	A value-at-risk approach to information security investments	Wang, J., Chaudhury, A., Rao, H.R.	2008	Inf. Syst. Res.	19	1	106-120	
25	An economic modelling approach to information security risk management	Bojanc R., Jerman-Blažič B.	2008	International Journal of Information Management				
26	BSI-Standard 100-2—IT-Grundschutz-Vorgehensweise	Bundesamt für Sicherheit in der Informationstechnik (BSI)	2008	online				
27	Cyber attacks: cross-country interdependence and enforcement	Wang, Q.-H., Kim, S.-H.	2009	Working Paper. National University of Singapore				
28	Why IT managers don't go for cyber-insurance products	Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C.	2009	Communications of the ACM	52	11	68-73	
29	Cyber insurance as an Incentive for Internet security	Bolot, J., & Lelarge, M.	2009	In Managing information risk and the economics of security (Springer US)			269-290	
30	Cyberattacks: does physical boundry matter?	Wang, Q.-H., Kim, S.-H.	2009	ICIS 2009 Proceedings			48	
31	Supporting cyber risk assessment of power control systems with experimental data	Dondossola, G., Garrone, F., & Szanto, J.	2009	Power Systems Conference and Exposition			1-3	
32	Cybersecurity Guide for Developing Countries	International Telecommunication Union	2009	online				
33	New cyber risk: premises for an insurance coverage	Addessi, M. E., Annibali, A., & Barracchini, C.	2009	International Review of Business Research Papers	5	6	50-62	
34	A taxonomy of operational cyber security risks	Cebula, J. J. and Young, L.R.	2010	Technical Note CMU/ SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.				

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	http://www.pitt.edu/~dtipper/2825/CIn.pdf	Academia	Finance / Insurance / RM	Qualitative	Risk Assessment	Asymmetric Information, Self Protection, Risk Accumulation, Externalities	
	http://www.sciencedirect.com/science/article/pii/S0019057807000754	Academia	IT	Qualitative	Risk Assessment	Risk Accumulation	SCADA, DCS, Risk analysis, Vulnerability assessment, Control systems
	http://digitalcommons.bryant.edu/cisjou/13/	Academia	Finance / Insurance / RM	Empirical	Risk Assessment		
	http://www.sciencedirect.com/science/article/pii/S026840120800039X	Academia	Economics	Theoretical	Risk Management (Mitigation / Insurance)	IT security	ICT security tools; Risk management; Technology investment
	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile&v=1 http://weis09.infosecon.net/files/153/	Industry	IT	Qualitative	Risk Management (Mitigation / Insurance)	Operational Cyber Risk, Regulation, IT Security	
		Academia	Finance / Insurance / RM	Empirical	Risk Assessment	Risk Modelling, Regulation, Risk Accumulation	
	http://dl.acm.org/citation.cfm?id=1592780	Academia	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Asymmetric Information, Pricing, Cyber Insurance	
	http://www.di.ens.fr/~lelarge/papiers/2008/cyber-surv.pdf	Academia	Finance / Insurance / RM	Theoretical	Risk Management (Mitigation / Insurance)	Self Protection, Risk Modelling, Networks	
	http://aisel.aisnet.org/icis2009/48/	Academia	Finance / Insurance / RM	Empirical	Risk Assessment	IT Security, Cyber Attacks, Interdependent Risks, Risk Accumulation	
	http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4840170&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4840170 http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf	Industry	IT	Qualitative	Risk Assessment		failure analysis power system control
		Industry	Economics	Qualitative	Risk Management (Mitigation / Insurance)		
	http://www.bizresearchpapers.com/4.Carla.pdf	Academia	Finance / Insurance / RM	Theoretical	Risk Assessment	Risk Modelling	Computer virus, worm, trojan, cyber risk, insurance
	http://www.sei.cmu.edu/reports/10tn028.pdf	Academia	IT	Qualitative	Risk Identification	Risk Taxonomy	

ID	Title	Author(s)	Year	Journal	Volume	Issue/ No.	Pages	
35	The global cybercrime industry	Kshetri, N.	2010	Springer				
36	Heavy-tailed distribution of cyber-risks	Maillart, T., and Sornette, D.	2010	The European Physical Journal	75		357-364	
37	Global risk report 2010—a global risk network report	World Economic Forum	2010					
38	Managing risk in information systems	Gibson, D.	2010	Jones & Bartlett Learning, Sudbury				
39	Competitive cyber-insurance and internet security	Shetty, N., Schwartz, G., Felegyhazi, M., & Walrand, J.	2010	Economics of Information Security and Privacy (Springer US)			229-247	
40	A model to analyze the unfulfilled promise of cyber insurance: the impact of secondary loss	Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C.	2010	Working paper				
41	Cyberwar: concept, status quo, and limitations	Myriam, D. C.	2010	Analysis in Security Policy	71			
42	Modeling cyber-insurance: Towards a unifying framework	Böhme and Schwartz	2010	Workshop on the Economics of Information Security (WEIS)				
43	Interdependent risk networks: the threat of cyber attack	Hofmann, A. and Ramaj, H.	2011	International Journal of Management and Decision Making	11	5	312–323	
44	Cyber security risk management: public Policy implications of correlated risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection	Ögüt, H., Raghunathan, S., and Menon, N.	2011	Risk Analysis	31	3	497–512	
45	Copula-based actuarial model for pricing cyber-insurance policies	Herath, H.S.B., Herath, T.C.	2011	Analyses and Actuarial Computations	2	1	7-20	

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	http://www.springer.com/de/book/9783642115219	Academia	Economics	Theoretical	Risk Identification	Cybercrime	
	http://arxiv.org/abs/0803.2256	Academia	Finance / Insurance / RM	Empirical	Risk Assessment	Risk Modelling, Data breach	
	http://www.weforum.org/pdf/globalrisk/globalrisks2010.pdf	Industry	Politics				
	http://www.jblearning.com/catalog/9781284055955/	Industry	IT	Qualitative	Risk Management (broad sense)		
	http://www.eecs.berkeley.edu/~schwartz/InsuranceMissing.pdf	Academia	Economics	Theoretical	Risk Assessment	IT Security, Externalities, Asymmetric Information	Cyber Insurance, Interdependent Security, Asymmetric Information, Network Externalities
	http://www.utdallas.edu/~rrao/CyberBMR[1].pdf	Academia	Finance / Insurance / RM	Theoretical	Risk Management (Mitigation / Insurance)	Asymmetric Information, Pricing, Insurability	
	http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analyses-71.pdf	Academia	Politics	Qualitative	Risk Identification	Cyberwar	
	http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf	Academia	IT	Theoretical	Risk Assessment	Risk Modelling	
	http://www.inderscienceonline.com/doi/abs/10.1504/IJMDM.2011.043406?journalCode=i-jmdm	Academia	Economics	Theoretical	Risk Identification	Externalities, Risk Accumulation	cyber harassment, cyber risk, cyber attack, cyber networks, cyber risk protection, cyber security, economic model, inter-dependencies, interdependent risks, information network, positive externalities, public goods
	http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2010.01478.x/pdf	Academia	Economics	Theoretical	Risk Management (Mitigation / Insurance)	Cyber Insurance, Self Protection, Externalities, Asymmetric Information	Cyber security; insurance; risk management
	http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1771983	Academia	Finance / Insurance / RM	Theoretical	Risk Assessment	Pricing, Risk Accumulation	Cyber-Insurance, Copula, Correlated Risk, Information Security Risk Management

ID	Title	Author(s)	Year	Journal	Volume	Issue/ No.	Pages	
46	Quantitatively assessing and visualising industrial system attack surfaces	Leverett, E. P	2011	University of Cambridge, Darwin College				
47	The UK cyber security strategy :protecting and promoting the UK in a digital world	Cabinet Office	2011	online				
48	Future global shocks: improving risk governance	OECD Reviews of Risk Management Policies	2011	online				
49	Incentives and barriers of the cyber insurance market in Europe	ENISA	2012					
50	10 Steps to Cyber Security	Government Communications Headquarters (GCHQ)	2012	White Paper of the Information Security Arm of GCHG				
51	Should your firm invest in cyber risk insurance?	Shackelford, S. J.	2012	Business Horizon	55		349–356	
52	COBIT 5. A business framework for the governance and management of enterprise IT	COBIT	2012					
53	The Cyber security threat to U.S. growth and prosperity	Dowdy, J.	2012	Aspen Strategy Group; in: Securing Cyberspace: A New Domain for National Security (eds. Burns, N., and Price, J.)				
54	General data protection regulation	European Commission	2012					

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	https://scadahacker.com/library/Documents/White_Papers/Univ%20of%20Cambridge%20-%20Assessing%20and%20Visualizing%20Industrial%20Attack%20Surfaces.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf	Academia	IT	Empirical	Risk Identification	DoS Attack	
	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf	Industry	Law	Qualitative	Risk Management (broad sense)	Regulation	
	http://www.oecd.org/governance/48329024.pdf	Industry	Trend studies	Qualitative	Risk Identification		
	https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe https://www.cyberessentials.org/system/resources/W1siZiIsIjIwMTQvMDYvMDQvMTdfNDdfMTdfNjMwXzEwX3N0ZXBzX3RvX2N5YmVyX3NlY3VyaXR5LnBkZiJdX/Q/10-steps-to-cyber-security.pdf http://www.sciencedirect.com/science/article/pii/S0007681312000377	Industry				Cyber Insurance	
		Industry		Qualitative			
		Academia	Management	Qualitative	Risk Management (Mitigation / Insurance)	Cyber Insurance, Data breach, Cyber Attachs, Systemic Risk, Data breach	Cybersecurity; Internet; Cyber risk insurance; Cyber attack; Data breach
	http://www.isaca.org	Industry	Management	Qualitative	Risk Management (Mitigation / Insurance)		
	http://www.mckinsey.com/our-people/john-dowdy	Industry	Economics	Qualitative			
	http://ec.europa.eu/justice/data-protection/reform/index_en.htm UriServ.do?uri=COM:2012:0011:FIN:EN:PDF (2012) http://www.munichre.com/de/reinsurance/magazine/publications/knowledge-series/technology-engineering-risks/cyberrisks/index.html http://www.sciencedirect.com/science/article/pii/S0305048311000582	Industry	Politics				

ID	Title	Author(s)	Year	Journal	Volume	Issue/ No.	Pages	
55	Cyberrisiken. Herausforderungen, Strategien und Lösungen für Versicherer	Munich Re	2012	Knowledge Series. Technology, Engineering and Risks				
56	IT security planning under uncertainty for high-impact events	Rakes, T. R., Deane, J. K., & Rees, L. P.	2012	Omega	40	1	79-88	
57	Cyber security	European Commission	2012	online				
58	Information technology—security techniques—guidelines for cybersecurity	ISO	2012	online				
59	Cybersecurity policy making at a turning point, analysing a new generation of national cybersecurity strategies for the Internet economy	OECD Reviews of Risk Management Policies	2012	online				
60	Risk and responsibility in a hyperconnected world: pathways to global cyber resilience	World Economic Forum (WEF)	2012	online				
61	Measuring the cost of cybercrime	Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., and Savage, S.	2013	The Economics of Information Security and Privacy (Springer)	12		265-300	
62	The Betterley report—cyber/privacy insurance market survey 2013	Betterley	2013					
63	Global corporate IT security risks: 2013	Kaspersky Lab	2013					
64	e-Crime—Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz	Geschonnek *et al*.	2013	KPMG Forensic Services				
65	Cyber-risk decision models: to insure IT or not?	Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukan, S. K.	2013	Decision Support Systems	56	1	11–26	
66	Cyber risk	National Association of Insurance Commissioners (NAIC)	2013					

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
		Industry					
		Academia	IT	Theoretical	Risk Management (Mitigation / Insurance)	Self Protection, IT security	Decision making/ process Integer programming; Risk; Information systems
	http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf	Industry	Law	Qualitative	Risk Assessment		
	https://www.iso.org/obp/ui/#iso:std:44375:en	Industry	Management	Qualitative	Risk Management (Mitigation / Insurance)		
	http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf	Industry	Trend studies	Qualitative	Risk Identification	Regulation	
	http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Risk Accumulation	
	http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf	Academia	Economics	Empirical	Risk Identification	Cybercrime	
	http://betterley.com/samples/cpims13_nt.pdf	Industry		Data collection		Survey	
	www.kasperskycontenthub.com/presscenter/files/2013/10/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf	Industry				Survey	
	http://docplayer.org/2853972-Studie-e-crime-computerkriminalitaet-in-der-deutschen-wirtschaft-mit-kennzahlen-fuer-oesterreich-und-schweiz-forensic.html http://www.sciencedirect.com/science/article/pii/S0167923613001115	Industry				Survey	
		Academia	Management	Theoretical	Risk Management (Mitigation / Insurance)	Cyber Insurance, Pricing, Risk Modelling	Security breach; Cyber-risk; Cyber-insurance; Copula; Bayesian Belief Network; Premium; Utility models
	http://www.naic.org/cipr_topics/topic_cyber_risk.htm	Industry					

ID	Title	Author(s)	Year	Journal	Volume	Issue/ No.	Pages	
67	Managing cyber security as a business risk: cyber insurance in the digital age	Ponemon Institute	2013					
68	Cyber-Versicherungen haben eine große Zukunft	Behrends, J.	2013	Versicherungswirtschaft	2		24–25	
69	Managing cyber risk: the trifecta	Francis, T.	2013	Am. Agent. Brok.	85	8	28	
70	Assessing corporate reputational damage of data breaches: an empirical analysis	Sinanaj, G., Muntermann, J.	2013	Proceedings of the 26th International Bled eConference			78-89	
71	From information security to cyber security	Von Solms, R., van Niekerk, J.	2013	Comput. Secur.	38		97–102	
72	Meeting the cyber risk challenge	Harvard Business Review	2013	Harvard Business School Publishing				
73	Willis Fortune 500 cyber disclosure study	Willis	2013					
74	Globally networked risks and how to respond	Helbing	2013	Nature	497		51-59	
75	Cyber risk insurance: a discourse and preparatory guide	Drouin, D.	2013	SANS Institute 2004				
76	Cyber resiliency assessment: Enabling architectural improvement	Bodeau and Graubart	2013	online				

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	www.assets.fiercemarkets.com/public/newsletter/fiercehealthit/experian-ponemonreport.pdf	Industry		Data collection		Survey	
	http://www.aon.com/germany/risk-services/cyber_risiken/versicherungswirtschaft_02_2013.pdf http://connection.ebscohost.com/c/articles/89497476/managing-cyber-risk-trifecta	Industry	Management	Qualitative			
	http://connection.ebscohost.com/c/articles/89497476/managing-cyber-risk-trifecta	Industry	Management	Qualitative	Risk Management (Mitigation / Insurance)		
	http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1006&context=bled2013	Academia	Management	Empirical	Risk Monitoring	IT Security, Data Breach, Event Study, Reputation	
	http://www.sciencedirect.com/science/article/pii/S0167404813000801	Academia	IT	Qualitative	Risk Management (Mitigation / Insurance)		Information security; Cyber security; Cybersecurity; Cyber-Security; Computer security; Risk; Threat; Vulnerability
	http://www.computerweekly.com/blogs/public-sector/Meeting%20the%20Cyber%20Risk%20Challenge%20-%20Harvard%20Business%20Review%20-%20Zurich%20Insurance%20group.pdf	Industry		Data collection		Survey	
	http://www.willis.com/documents/publications/Services/Executive_Risks/2013/FinexNA_Cyber_Update_v2.pdf	Industry		Data collection		Survey	
	http://www.nature.com/nature/journal/v497/n7447/full/nature12047.html	Academia	IT	Theoretical	Risk Identification	Systemic Risk, Risk Accumulation	Socioeconomic scenarios Sustainability Complex networks
	http://citeseerx.ist.psu.edu/viewdoc/download?-doi=10.1.1.203.336&rep=rep1&-type=pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)		cyber risk management; security-related trade-off; cyber attack; mission impact; threat; vulnerability; countermeasure; attack space; expected loss
	https://www.mitre.org/sites/default/files/pdf/12_3795.pdf	Industry	IT	Qualitative	Risk Management (Mitigation / Insurance)	IT Security	

ID	Title	Author(s)	Year	Journal	Vol-ume	Issue/ No.	Pages	
77	Cyber-crime, securities markets and systemic risk	Tendulkar	2013	Joint Staff Working Paper, International Organization of Securities Commissions Research Department and World Federation of Exchanges				
78	Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector	United Nations (UN) Office on Drugs and Crime	2013	online				
79	Building resilience in supply chains	World Economic Forum (WEF)	2013	online				
80	Insurance—cyber risk	Willis	2013	online				
81	Profile of a macro-catastrophe threat type							
82	The extreme vulnerability of interdepen-dent spatially embedded networks	Bashan, A., Berezin, Y., Buldyrev, S. V., & Havlin	2013	Nature Physics	9	10	667-672	
83	The economic impact of cyber terrorism	Hua, J., & Bapna, S.	2013	The Journal of Strategic Information Systems	22	2	175-186	
84	Conflict and negotiation in cyberspace	James A. Lewis	2013	Center for Strategic and International Studies (CSIS)				
85	Tallinn manual on the international law applicable to cyber warfare	Schmitt, M. N.	2013	Cambridge University Press				
86	PAS 555 2013 cyber security risk governance and Management	British Standards Institution (BSI)	2013	online				

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf	Industry	Law	Data collection	Risk Identification	Survey	
	http://www.unodc.org/documents/organised-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf	Industry	Politics	Qualitative	Risk Assessment	Regulation	
	http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf	Industry	Management	Qualitative	Risk Management (Mitigation / Insurance)	Critical Infrastructure	
	http://www.pwc.dk/da/arrangementer/assets/cyber-tineolsen.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)		
	http://cambridgeriskframework.com/downloads	Academia	Finance / Insurance / RM	Data collection	Risk Identification	Risk Accumulation	Catastrophe, Scenario, Cyber, Risk, Threat, Vulnerability, Theft, Interruption, Damage, Magnitude
	http://arxiv.org/pdf/1206.2062.pdf	Academia	IT	Theoretical	Risk Identification	Networks, Risk Modelling, Interdependent Risks	EMBEDDED Internet devices,COMPUTER systems security vulnerabilities, LATTICE networks, ELECTRIC power distribution grids, INTERNET, COMPUTER network resources—Management.
	http://www.sciencedirect.com/science/article/pii/S0963868712000522	Academia	Economics	Theoretical	Risk Management (Mitigation / Insurance)	Cybercrime, IT Security, Risk Modelling,	Game theory; Information systems security; Security investment; Cyber terrorism
	https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130208_Lewis_Conflict-Cyberspace_Web.pdf https://ccdcoe.org/tallinn-manual.html	Industry	Politics	Qualitative	Risk Management (Mitigation / Insurance)	Cyberwar	
		Industry	Law	Qualitative	Risk Identification	Regulation, Cyberwar	
	http://www.itgovernance.co.uk/shop/p-1356-pas-555-2013-cyber-security-risk-governance-and-management-specification.aspx	Industry	Politics	Qualitative	Risk Management (Mitigation / Insurance)	IT Security, Self Protection	

ID	Title	Author(s)	Year	Journal	Volume	Issue/ No.	Pages	
87	Cyber security self-assessment guidance	Office of the Superintendent of Financial Institutions	2013	online				
88	Cyber liability—it's just a click away	Zelle, A. R., and Whitehead, S. M.	2014	Journal of Insurance Regulation	33		145-168	
89	The Betterley Report—cyber/privacy insurance market survey 2014	Betterley	2014					
90	A cloud security risk-management strategy	Choo, K. K. R.	2014	Cloud Computing, IEEE	1	2	52-56	
91	Cyber security—the risk of supply chain vulnerabilities in an enterprise firewall	Kuypers, M. A., Heon, G., Martin, P., Smith, J., Ward, K., and Paté-Cornell, E.	2014	Working Paper—Stanford University.				
92	historical development of cyber (re) insurance	Marsh	2014					
93	Net losses—estimating the global cost of cybercrime	McAfee	2014					
94	Cost of data breach study—global analysis	Ponemon Institute	2014					
95	Risky business—lessons for mitigating cyber attacks from the international insurance law on piracy	Shackelford, S., and Russell, S. L.	2014	Minnesota Journal of International Law Online (forthcoming)				
96	Working together with clients to find cyber risk solutions	Swiss Re	2014					

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx	Industry	Politics	Qualitative	Risk Management (Mitigation / Insurance)		
	http://www.naic.org/documents/prod_serv_jir_JIR-ZA-33-06-EL.pdf	Industry	Law	Qualitative	Risk Management (Mitigation / Insurance)	Data breach, Regulation, Contract Design	
	http://betterley.com/samples/cpims14_nt.pdf	Industry		Data collection		Survey	
	http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&tp=&arnumber=6924649	Academia	IT	Empirical	Risk Management (Mitigation / Insurance)	New Technologies	cloud computing, data privacy, government policies, security of data, cloud privacy cloud security risk-management strategy cloud service providers cyberthreats malicious cyberactivities organizational cloud service users organizational competitiveness public policy concerns security breaches
	http://psam12.org/proceedings/paper/paper_32_1.pdf	Academia	IT	Empirical	Risk Assessment	Risk Modelling, IT Security	Cyber security, Supply chain, risk analysis
	http://www.gccapitalideas.com/2014/10/23/historical-development-of-cyber-reinsurance/	Industry		Data collection		Survey	
	http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf	Industry		Data collection		Survey	
	http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/	Industry		Data collection		Survey	
	http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2509428	Academia	Law	Theoretical	Risk Management (Mitigation / Insurance)	Cyber Attachs, Cyber Insurance,Self Protection	cybersecurity, insurance, piracy, cyber attack, cyber threat, cyber risk insurance
	http://www.swissre.com/reinsurance/insurers/casualty/smarter_together/working_smarter_together_for_cyber-risk_solutions_in_EMEA.html	Industry					

ID	Title	Author(s)	Year	Journal	Volume	Issue/ No.	Pages	
97	Global risks report 2014—ninth edition	World Economic Forum	2014					
98	Die Cyber-Versicherung: Unerlässlicher Teil eines effektiven Risikomanagements	Behrends, J.	2014	St. Galler Trendmonitor für Risiko- und Finanzmärkte	1		13-16	
99	The UK cyber security strategy. Protecting and promoting the UK in a digital world	Cabinet Office	2014					
100	Der Cyber-Versicherungsmarkt in Deutschland, Eine Einführung	Choudhry, U.	2014	Springer Gabler Verlag, Wiesbaden				
101	Risiken aus der Nutzung von Cloud-Computing-Diensten: Fragen des Risikomanagements und Aspekte der Versicherbarkeit.	Haas, A., Hofmann, A.	2014	Zeitschrift für die gesamte Versicherungswissenschaft	103	4	377–407	
102	Cyber-Risiken. Marktentwicklung & Risikomanagement	Marsh	2014					
103	Risk nexus: beyond data breaches: global interconnections of cyber risk	Zurich	2014					
104	Cyber resilience—the cyber risk challenge and the role of insurance	CRO Forum	2014	online				
105	Cyber claims study	NetDiligence	2014	online				
106	Framework for improving critical infrastructure cybersecurity	U.S. National Institute of Standards and Technology (NIST)	2014	online				
107	Case study: critical controls that could have prevented Target breach	SANS Institute	2014	online				
108	Cyber essentials scheme: summary	Department for Business, Innovation & Skills and Cabinet Office	2014	online				
109	Cyber essentials scheme: requirements for basic technical protection from cyber attacks	Department for Business, Innovation & Skills and Cabinet Office	2014	online				
110	Assessment methodology for the oversight expectations applicable to critical service providers	Bank for International Settlements and International Organization of Securities Commissions (BIS)	2014	online				

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	http://www.weforum.org/reports/global-risks-2014-report	Industry	Politics				
		Industry	Management	Qualitative			
	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf	Industry	Law			Regulation	
	http://www.springer.com/us/book/9783658070977	Industry	Management	Qualitative	Risk Management (broad sense)		
	http://link.springer.com/search?query=Risiken+aus+der+Nutzung+von+Cloud-Computing-Diensten%3A+Fragen+des+Risikomanagements&search-within=Journal&facet-journal-id=12297	Academia	Management	Qualitative	Risk Identification	New Technologies, Insurability	
	https://www.lloyds.com/~/media/files/lloyds/offices/german/cyber%20risks%20frankfurt%202014/marsh-cyber%20risks%20vortraglloyds%20frankfurt12022014.pdf	Industry					
	http://www.atlanticcouncil.org/publications/reports/beyond-data-breaches-global-interconnections-of-cyber-risk	Industry			Risk Assessment	Risk Accumulation	
	http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Risk Taxonomy, Cyber Insurance, Insurability	
	http://www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf	Industry	Finance / Insurance / RM	Data collection	Risk Assessment	Data Breach, Underwriting Cyber Risk, Data Collection	
	http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Regulation	
	https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Phishing Attacks	
	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf	Industry	Law	Qualitative	Risk Management (Mitigation / Insurance)	Regulation	
	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf	Industry	Law	Qualitative	Risk Management (Mitigation / Insurance)	Regulation, IT Security	
	http://www.bis.org/cpmi/publ/d123.pdf	Industry	Law	Qualitative	Risk Management (Mitigation / Insurance)	Regulation	

ID	Title	Author(s)	Year	Journal	Vol-ume	Issue/ No.	Pages	
111	Principles for effective cybersecurity regulatory guidance	Securities Industry and Financial Markets Association	2014	online				
112	Cyber risks & exposures	Lloyd's	2014	online				
113	Achieving cyber resilience	AIG	2014	online				
114	Cyber-risk oversight	National Association of Corporate Directors (NACD)	2014	online				
115	Schadenspiegel: Gefahr aus dem Netz	Munich Re	2014	Das Magazin für Schadenmanager				
116	2014 Emerging risk acumen: key findings	AXA	2014	online				
117	Cyber risk—a global systemic threat	DTCC	2014	online				
118	IRM'S cyber risk executive summary	Institute of Risk Manage-ment	2014	online				
119	Stress test scenario—Sybil Logic Bomb cyber catastrophe	Ruffle, S.J.; Bowman, G.; Caccioli, F.; Coburn, A.W.; Kelly, S.; Leslie, B.; Ralph, D.; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.	2014	online				
120	Markets for cybercrime tools and stolen data: hackers' bazaar	Ablon, L., Libicki, M. C., & Golay, A. A.	2014	National Security Research Division (RAND)				
121	Strategies to mitigate targeted cyber intrusions	AUSTRALIAN SIGNALS DIRECTORATE (ASD)	2014	online				

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	http://www.sifma.org/issues/item.aspx?id=8589951691	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)		
	http://www.lloyds.com/~/media/files/the%20market/communications/market%20bulletins/2014/11/y4842.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Monitoring		
	https://www.aig.com/content/dam/aig/america-canada/us/documents/insights/1158y-achieving-cyber-resilience-brochure.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Operational Cyber Risk, IT security	
	https://www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687	Industry	Management	Qualitative	Risk Management (Mitigation / Insurance)	Operational Cyber Risk, IT security	
	http://www.munichre.com/site/corporate/get/documents_E-2068517148/mr/assetpool.shared/Documents/5_Touch/_Publications/302-08481_de.pdf	Industry	Management	Qualitative			
		Industry	Finance / Insurance / RM	Qualitative	Risk Identification		
	http://www.google.ch/url?sa=t&rct=-j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi1iY-6_4bNAhXFWBoKHf3VCfUQFggiMAA&url=http%3A%2F%2Fwww.dtcc.com%2F~%2Fmedia%2FFiles%2FDownloads%2Fissues%2Frisk%2Fcyber-risk.pdf&usg=AFQjCNHaLHeWuZLVBLjiw_2JwBAUCh4xPA	Industry	Politics	Qualitative	Risk Identification	Systemic Risk, Interdependent Risks	
	https://www.theirm.org/media/883443/Final_IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)		
	http://cambridgeriskframework.com/downloads	Academia	Economics	Qualitative	Risk Identification	Critial Infrastructure, Systemic Risk, Risk Accumulation, Risk Modelling	
	http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf	Academia	Economics	Empirical	Risk Identification	Cybercrime	Computer Viruses, Cybercrime, Health Information Privacy, Information Security, The Internet, Law Enforcement, Markets
	http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf	Industry	Politics	Qualitative	Risk Management (Mitigation / Insurance)	IT Security, Self Protection	

ID	Title	Author(s)	Year	Journal	Volume	Issue/ No.	Pages	
122	Cyber risk: nightmare or opportunity	RMProfessional	2014	online				
123	Monitoring IT operational risks across U.S. capital markets	Friedhoff, J. and Mansouri, M.	2015	Journal of Operational Risk	10	2		
124	Insurability of Cyber Risk: An Empirical Analysis	Biener, C., Eling, M., and Wirfs, J.H.	2015	The Geneva Papers	40	1	131-158	
125	Insurance for cyber risks—a comprehensive analysis of the evolving exposure, today's litigation, and tomorrow's challenges	Podolak, G.D.	2015	Quinnipiac Law Review	33		369-409	
126	Cyber risk insights conference	Advisen	2015					
127	A guide to cyber risk—managing the impact of increasing Interconnectivity	Allianz Global Corporate & Specialties (AGCS)	2015					
128	The Betterley report—cyber/privacy insurance market survey 2015	Betterley	2015					
129	Modelling and management of cyber risk	Eling, M. and Wirfs, J. H.	2015	Working Paper				
130	Business blackout—The insurance implications of a cyber attack on the US power grid.	Lloyd's	2015					
131	Promoting UK cyber prosperity: public–private cyber-catastrophe Reinsurance.	Long Finance	2015					
132	European 2015 cyber risk survey report	Marsh	2015					
133	Share of companies with standalone cyber insurance in the United States from 2013 to 2014, by industry	Statista	2015	online				
134	The extreme risk of personal data breaches and the erosion of privacy	Wheatley, S., Maillart, T., and Sornette, D.	2015	Working Paper—Cornell University Library				
135	Optimal risk transfer for cyber risk	Wirfs, J. H.	2015	Working Paper				
136	Global risks report 2015—tenth edition	World Economic Forum	2015					

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	https://www.theirm.org/media/984144/cyber_risk_article_for-web.pdf	Industry	IT	Qualitative	Risk Management (Mitigation / Insurance)	IT Security, Self Protection	
	http://www.risk.net/journal-of-operational-risk/technical-paper/2413196/monitoring-it-operational-risks-across-us-capital-markets	Academia	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Regulation	
	http://www.palgrave-journals.com/gpp/journal/v40/n1/abs/gpp201419a.html	Academia	Finance / Insurance / RM	Empirical	Risk Management (broad sense)	Data collection, Risk Modelling, Cyber Insurance, Risk Accumulation	Cyber risk; cyber insurance; operational risk; insurability
	https://www.qu.edu/prebuilt/pdf/SchoolLaw/LawReviewLibrary/Vol33_Issue2_2015_podolak.pdf	Academia	Law	Qualitative	Risk Management (Mitigation / Insurance)	Contract Design, Regulation	
	http://www.advisenltd.com/wp-content/uploads/london-cyber-risk-insights-conference-slides-2015-02-17.pdf	Industry					
	http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRisk-Guide.pdf	Industry			Risk Management (Mitigation / Insurance)	Risk Accumulation	
	http://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf	Industry		Data collection		Survey	
	http://www.actuaries.org/oslo2015/papers/IAALS-Wirfs&Eling.pdf	Academia	Finance / Insurance / RM	Empirical	Risk Assessment	Risk Modelling, Risk Accumulation	Cyber risk, risk management, insurance
	https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout	Industry					
	http://www.longfinance.net/images/Promoting_UK_Cyber_Prosperity_28July2015.pdf	Industry					
	http://uk.marsh.com/Portals/18/Documents/European%202015%20Cyber%20Risk%20Survey%20Report-10-2015.pdf.	Industry		Data collection		Survey	
	http://www.statista.com/statistics/424166/share-of-companies-with-cyber-insurance-usa-by-industry/	Industry		Data collection	Risk Identification		
	http://arxiv.org/abs/1505.07684	Academia	Finance / Insurance / RM	Empirical	Risk Assessment	Data breach, Risk Modelling	
		Academia	Finance / Insurance / RM	Empirical	Risk Management (Mitigation / Insurance)		
	http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf	Industry	Politics				

ID	Title	Author(s)	Year	Journal	Vol-ume	Issue/ No.	Pages	
137	Cyber Risk: Risikomanagement und Versicherbarkeit	Biener, C., Eling, M., Matt, A. and Wirfs, J.H.	2015	I-VW HSG Schriftenreihe	54			
138	Components and challenges of integrated cyber risk management	Kosub. T.	2015	ZVersWiss	104		615-634	
139	Hype and heavy tails—a closer look at data breaches	Edwards, B., Hofmeyr, S. and Forrest, S.	2015	Working Paper				
140	Cyber-risk management	Refsdal, A., Solhaug, B., & Stølen, K	2015	Springer International Publishing				
141	Cybersecurity assessment tool	Federal Financial Institutions Examination Council (FFIEC)	2015	online				
142	Insurance banana skins	Centre for the Study of Financial Innovation (CSFI) / PwC	2015	online				
143	Managing cyber risks in an interconnected world—key findings from The Global State of Information Security® Survey 2015	PwC	2015	online				
144	2015 Data Breach Investigations Report	Verizon	2015	online				
145	2015 cost of data breach study—global analysis	Ponemon Institute	2015	online				
146	Network and information security directive: co-legislators agree on the first EU-wide legislation on cybersecurity	European Commission	2015	online				
147	New data protection standards to ensure smooth police cooperation in the EU	European Parliament	2015	online				
148	Cyber essentials scheme: assurance framework	Department for Business, Innovation & Skills and Cabinet Office	2015	online				

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	http://www.ivw.unisg.ch/de/forschung/anwendungsorientierte+-forschung/schriftenreihe	Academia	Finance / Insurance / RM	Empirical	Risk Assessment		
	http://www.google.ch/url?sa=t&rct=-j&q=&esrc=s&source=web&cd=1&-cad=rja&uact=8&ved=0ahUKEwi-jzdrO_obNAhUDXhoKHX_KDKYQF-gggMAA&url=http%3A%2F%2Flink.springer.com%2Farticle%2F10.1007%252Fs12297-015-0316-8&usg=AFQ-jCNGvPJf8LVFFxvq6l1Hp4JGw-orU-KA&sig2=4dOWBE9xAWqc	Academia	Management	Qualitative	Risk Management (broad sense)		
	http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_ed-wards.pdf	Academia	Finance / Insurance / RM	Empirical	Risk Assessment	Data Breach, Risk Modelling	
	http://link.springer.com/book/10.1007/978-3-319-23570-7	Academia	Finance / Insurance / RM	Qualitative	Risk Management (broad sense)		
	https://www.ffiec.gov/pdf/cybersecu-rity/FFIEC_CAT_June_2015_PDF2.pdf	Industry	Management	Qualitative	Risk Identification		
	http://static1.squarespace.com/static/54d620fce4b049bf4cd-5be9b/t/55dde0fce4b0d ff-05004146c/1440604412304/2015+-Insurance+Banana+Skins+FINAL.pdf	Industry	Finance / Insurance / RM	Data collection	Risk Identification	Survey	
	https://www.pwc.ch/de/dyn_output.html?content.void=57078&col-lectionpageid=8240&con-tainervoid=46459&comef-romcontainer=true	Industry	Finance / Insurance / RM	Data collection	Risk Assessment	Survey	
	http://www.verizonenterprise.com/DBIR/2015/	Industry	Finance / Insurance / RM	Data collection	Risk Assessment	Survey	
	http://www-03.ibm.com/security/data-breach/	Industry	Finance / Insurance / RM	Data collection	Risk Assessment	Survey	
	https://ec.europa.eu/digital-sin-gle-market/news/network-and-in-formation-security-directive-co-leg-islators-agree-first-eu-wide-legislation	Industry	Law	Qualitative	Risk Management (broad sense)	Regulation	
	http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2f-TEXT%2bIM-PRESS%2b20151217I-PR08122%2b0%2bDOC%2bXM-L%2bV0%2f%2fEN&language=EN	Industry	Law	Qualitative	Risk Management (broad sense)	Regulation	
	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400914/bis-15-72-cyber-essentials-scheme-assurance-framework.pdf	Industry	Law	Qualitative	Risk Management (Mitigation / Insurance)	Regulation	

ID	Title	Author(s)	Year	Journal	Vol-ume	Issue/ No.	Pages	
149	Principles for effective cybersecurity: insurance regulatory guidance	National Association of Insurance Commissioners (NAIC)	2015	online				
150	Project2020: scenarios for the future of cybercrime	International Cyber Security Protection Alliance (ICSPA)	2015	online				
151	Digital security risk management for economic and social prosperity	OECD	2015	online				
152	Cyber-security risks in the supply chain	UK National Computer Emergency Response Team	2015	online				
153	Partnering for cyber resilience—towards the quantification of cyber threats	World Economic Forum (WEF)	2015	online				
154	A quick guide to cyber risk	Lloyd's	2015	online				
155	Cyber core data requirements	Lloyd's	2015	online				
156	Market bulletin: cyber-attack: managing catastrophe-risk and exposures	Lloyd's	2015	online				
157	The Internet of Things is already here, but who bears the risks? A model to explain coverage disputes in a world of interconnected, autonomous devices	Haas, A., Haas, M., & Weinert, M.	2015	Working paper				
158	Drive-bys, spear-phishing and Trojans—the changing face of cyber security	Wüest C.	2015	Swiss Re Centre of Global Dialogue				
159	Has 'big data' become 'too big'?`	AXA	2015	online				
160	Cyber risk: thread and opportunity	Hartwig & Wilkinson	2015	Insurance Information Institute				
161	Cyber war: the next threat to national security and what to do about it?	Clarke, R. A. and Knake, R. K.	2015	Strategic Analysis	39	4	458-460	
162	Unique in the shopping mall: on the reidentifiability of credit card metadata	De Montjoye, Y. A., Radaelli, L., & Singh, V. K.	2015	Science	347	6221	536-539	
163	Technology: bitcoin	Lloyd's	2015	online				

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf	Industry	Law	Qualitative	Risk Management (broad sense)	Regulation	
	https://www.icspa.org/wp-content/uploads/2015/03/ICSPA_Project_2020_-_Scenarios_for_the_Future_of_Cybercrime.pdf	Industry	Trend studies	Qualitative	Risk Identification		
	http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf	Industry	Economics	Qualitative	Risk Management (broad sense)		
	https://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf	Industry	Management	Qualitative	Risk Management (broad sense)	Critical Infrastructure	
	http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Assessment	Risk Modelling	
	https://www.lloyds.com/news-and-insight/news-and-features/emerging-risk/emerging-risk-2015/a-quick-guide-to-cyber-risk	Industry	Management	Qualitative	Risk Management (Mitigation / Insurance)	Cyber Insurance	
	http://www.lloyds.com/news-and-insight/risk-insight/emerging-risks-team/cyber-core-data-requirements	Industry	Finance / Insurance / RM	Qualitative	Risk Identification	Risk Taxonomy	
	https://www.lloyds.com/~/media/files/the%20market/communications/market%20bulletins/2015/11/y4938.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Monitoring		
	http://www.wriec.net/wp-content/uploads/2015/07/6J3_Haas.pdf	Academia	Finance / Insurance / RM	Theoretical	Risk Management (Mitigation / Insurance)	Externalities, IT Quality, Risk Modelling	Internet of Things, cyber insurance, insurance, risk bearing, startups
	http://media.cgd.swissre.com/documents/Cyber_security_Wuest_RDM_September11.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Identification		
	https://www.axa.com/en/spotlight/story/big-data	Industry	Finance / Insurance / RM	Qualitative	Risk Identification	New Technologies	
	http://www.iii.org/sites/default/files/docs/pdf/cyber_risk_wp_final_102015.pdf	Industry	Finance / Insurance / RM	Data collection	Risk Identification	Data Breach	
	http://www.tandfonline.com/doi/full/10.1080/09700161.2015.1047221	Industry	Politics	Qualitative	Risk Identification	Cyber War	
	http://science.sciencemag.org/content/347/6221/536	Academia	IT	Empirical	Risk Identification		
	https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/bitcoin%20%20final.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Assessment	New Technologies	

ID	Title	Author(s)	Year	Journal	Vol-ume	Issue/ No.	Pages	
164	Risk nexus: overcome by cyber risks? Economic benefits and costs of alternate cyber futures	Zürich	2015	online				
165	Risk nexus: global cyber governance: preparing for new business risks	Zürich	2015	online				
166	2015 cyber security and data privacy survey: how prepared are you?	Dena Cusick	2015	White paper				
167	IBM 2015 Cyber Security Intelligence index	IBM	2015	online				
168	The Internet organised crime threat assessment	EUROPOL	2015	online				
169	Cyber risk handbook 2015	Marsh & McLennan	2015	online				
170	Information security and cyber liability risk management	Advisen & Zürich	2015	online				
171	OCIE's 2015 Cybersecurity Examination Initiative	Office of Compliance Inspections and Examina-tions (OCIE)	2015	online				
172	The cyber insurance multi-year plan	PwC	2015	online				
173	Cross sector—global: cyber risk of growing importance to credit analysis	Moody's	2015	online				
174	Cyber risk and corporate credit	Standard & Poor's	2015	online				
175	Topics risk solutions: reputations under attack	Munich Re	2015	online				
176	S&P: US-Versicherer haben Cybersparte im Griff	Herbert Frommes Versicherungsmonitor	2015	online				
177	VdS Quick-Audit für Cyber-Security: Verfahren	VdS Schadenverhütung GmbH	2015	online				

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	http://publications.atlanticcouncil.org/cyberrisks	Industry	Trend studies	Qualitative	Risk Assessment		
	http://itemsweb.esade.edu/wi/web/risk-nexus-april-2015-global-cyber-governance.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Management (broad sense)	New Technol-ogies	
	https://wfis.wellsfargo.com/insights/research/2015-Cyber-Security-and-Data-Privacy-Survey/Documents/Cyber_data_privacy_survey_white_paper_FNL.pdf	Industry	Finance / Insurance / RM	Empirical	Risk Management (Mitigation / Insurance)	Survey, Cyber Insurance	
	https://essextec.com/wp-content/uploads/2015/09/IBM-2015-Cyber-Security-Intelligence-Index_FULL-REPORT.pdf	Industry	IT	Empirical	Risk Assessment	Cyber Attachs, Data Collection	
	https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015	Industry	Politics	Qualitative	Risk Management (broad sense)	Cybercrime	
	http://www.curie.org/sites/default/files/2015Cyber%20Risk%20Handbook-10-2015.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Management (broad sense)		
	http://www.advisenltd.com/wp-content/uploads/2015/10/information-security-cyber-liability-risk-management-report-2015-10-16.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Cyber Insurance, Survey,	
	https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf	Industry	Politics	Qualitative	Risk Management (Mitigation / Insurance)		
	http://pwc.blogs.com/north/2015/03/the-cyber-insurance-multi-year-plan-.html	Industry	Finance / Insurance / RM	Qualitative	Risk Management (broad sense)	Cyber Insurance	
	https://www.moodys.com/registerinfo.aspx?registerButtonclicked=true&-from=Doc_Reg	Academia	Management	Qualitative	Risk Assessment	Rating	
	http://www.maalot.co.il/publications/OAC20150708094842.pdf	Industry	Management	Qualitative	Risk Assessment	Rating	
	https://www.munichre.com/site/templeinsurance/get/documents_E1131510054/mroc/assetpool.templeinsurance/Documents/3.%20Publications/302-08554_en.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Reputation, Insurability, Cyber Insurance	
	http://versicherungsmonitor.de/2015/06/sp-us-versicherer-haben-cybersparte-im-griff/	Industry	Finance / Insurance / RM	Qualitative	Risk Assessment	Rating, Underwriting Cyber Risk, Cyber Insurance	
	http://versicherungsmonitor.de/2015/06/sp-us-versicherer-haben-cybersparte-im-griff/	Industry	Finance / Insurance / RM	Qualitative	Risk Assessment	Rating, Underwriting Cyber Risk, Cyber Insurance	

ID	Title	Author(s)	Year	Journal	Vol-ume	Issue/ No.	Pages	
178	VdS 3473en—cyber security for small and medium enterprises, Requirements	VdS Schadenverhütung GmbH	2015	online				
179	VdS 5555en—cyber security for small and medium enterprises, Brochure	VdS Schadenverhütung GmbH	2015	online				
180	Cyber risk: too big to insure? risk transfer options for a mercurial risk class	Eling M., Wirfs J.H.	2016	Institute of Insurance Economics I.VW-HSG, University of St. Gallen				
181	Issues paper on cyber risk to the insurance sector	IAIS (International Association of Insurance Supervisors)	2016	online				
182	DataLossDB		2016	online				
183	Fact sheet: cybersecurity national action plan	The Withe House	2016	online				
184	Cyber insurance exposure data schema V1.0	Cambridge Centre for Risk Studies	2016	online				
185	Cyber exposure data standard and preparer's guide	AIR Worldwide						
186	Cyber risks spill over into the physical world	Zürich	2016	online				
187	Recommendations for public–private partnership against cybercrime	World Economic Forum (WEF)	2016	online				
188	The benefits and limits of cyber value-at-risk	Deloitte	2016	online				
189	Ukraine attack highlights cyber-risk to critical infrastructure	Zürich	2016	online				
190	Mitigating the inevitable:how organizations manage data breach EXPOSURES	Advisen	2016	online				

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	https://vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf	Industry	IT	Qualitative	Risk Management (Mitigation / Insurance)	Operational Cyber Risk, Self Protection, IT Security	
	https://vds.de/fileadmin/vds_publikationen/vds_5555en_web.pdf	Industry	IT	Qualitative	Risk Management (Mitigation / Insurance)	Operational Cyber Risk, Self Protection, IT Security	
	http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf	Academia	Finance / Insurance / RM	Empirical	Risk Management (broad sense)		
	http://www.iaisweb.org/page/news/consultations/current-consultations/issues-paper-on-cyber-risks-to-the-insurance-sector//file/60062/issues-paper-on-cyber-risk-to-the-insurance-sector-public-consultation	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Cybercrime, Operational Cyber Risk, Regulation, Risk Taxonomy	
	https://blog.datalossdb.org/	Industry		Data collection	Risk Identification	Data Breach, Data Collection	
	https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan	Industry	Law	Qualitative	Risk Management (broad sense)	Regulation	
	http://cambridgeriskframework.com/getdocument/38	Industry	Finance / Insurance / RM	Qualitative	Risk Identification	Risk Taxonomy	
	http://www.air-worldwide.com/Documentation/Cyber-Exposure-Data-Standard/Index.htm	Industry	Finance / Insurance / RM	Qualitative	Risk Identification	Risk Taxonomy	
	https://www.zurich.com/en/knowledge/articles/2016/04/cyber-risks-spill-over-into-the-physical-world	Industry	Management	Qualitative	Risk Assessment	Risk Accumulation	
	https://www.zurich.com/_/media/dbe/corporate/docs/whitepapers/wef-cybercrime-recommendations.pdf?la=en	Industry	Politics	Qualitative	Risk Management (Mitigation / Insurance)	Regulation	
	https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-benefits-limits-cyber-value-at-risk-03032016.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Assessment		
	https://www.zurich.com/en/knowledge/articles/2016/03/ukraine-attack-highlights-cyber-risk-to-critical-infrastructure	Industry	Management	Qualitative	Risk Identification	Critical Infrastructure	
	http://www.advisenltd.com/wp-content/uploads/2016/03/how-organizations-manage-data-breach-exposures-2016-03-03.pdf	Industry	Management	Qualitative	Risk Management (Mitigation / Insurance)	Operational Cyber Risk, Data breach	

ID	Title	Author(s)	Year	Journal	Vol-ume	Issue/ No.	Pages	
191	Companies still unprepared for mounting cyber risks	Zürich	2016	online				
192	Allianz Risk Barometer Top Business Risks 2016	Allianz Global Corporate & Specialties (AGCS)	2016	online				
193	Data protection and the cloud meeting growing security needs	SCOR	2016	online				
194	Searching for stability in cyber space	Berkshire Hathaway Specialty Insurance	2016	Risk and Insurance				
195	UK: businesses don't believe they are at risk of cybercrime	Aviva	2016	online				
196	Environmental cyber risk White Paper	XL Group plc	2016	online				
197	Staying ahead of emerging cyber risks	XL Group plc	2016	online				
198	Technology and cyber risk liability	XL Group plc	2016	online				
199	Cyber claim trend: risks go beyond data breaches	XL Group plc	2016	online				
200	2016 Internet security threat report	Symantec Company	2016	online				
201	Managing cyber insurance accumulation risk	Risk Management Solutions, Inc.,report prepared in collaboration with and based on original research by the Centre for Risk Studies,University of Cambridge.	2016	online				
202	Integrated infrastructure: cyber resiliency in society	Kelly, S.; Leverett, E.; Oughton, E. J.; Copic, J.; Thacker, S.; Pant, R.; Pryor, L.; Kassara, G.; Evan, T.; Ruffle, S. J.;Tuveson, M.; Coburn, A. W.; Ralph, D. & Hall, J. W.; Cambridge Risk Framework series; Centre for Risk Studies, Uiversity of Cambridge.	2016	online				
203	IRGC workshop on comparing methods for terrorism risk assessment with methods in cyber security	International Risk Governance Council (IRGC)	2016	online				

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	https://www.zurich.com/en/knowledge/articles/2016/03/companies-still-unprepared-for-mounting-cyber-risks	Industry	Management	Qualitative	Risk Management (broad sense)		
	http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf	Industry	Management	Qualitative	Risk Identification		
	https://www.scor.com/images/stories/pdf/library/SCORviews/Sv0316-Rodgers.pdf	Industry	IT	Qualitative	Risk Management (Mitigation / Insurance)	New Technologies	
	http://www.bhspecialty.com/Cyber%20R&I%20PDF%20-%20BHSI%20-%2004_18_2016.pdf	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)		
	http://www.aviva.com/media/news/item/uk-businesses-dont-believe-they-are-at-risk-of-cyber-crime-says-aviva-17582/	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)		
	http://xlcatlin.com/search?q=cyber+risk&slang=en	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Critical Infrastructure	
	http://xlcatlin.com/search?q=cyber+risk&slang=en	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)		
	http://xlcatlin.com/search?q=cyber+risk&slang=en	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)		
	http://xlcatlin.com/search?q=cyber+risk&slang=en	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)		
	https://www.symantec.com/security-center/threat-report	Industry	IT	Data collection	Risk Identification	Data Breach, Data Collection, Survey	
	http://cambridgeriskframework.com/downloads	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Critial Infrastructure, Systemic Risk, Risk Accumulation, Risk Modelling	
	http://cambridgeriskframework.com/downloads	Academia	Economics	Data collection	Risk Identification	Critial Infrastructure, Systemic Risk, Risk Accumulation, Risk Modelling	
	https://www.irgc.org/event/terrorism-cybersecurity-workshop/	Industry	Finance / Insurance / RM	Qualitative	Risk Management (broad sense)	Cyber Terrorism	

ID	Title	Author(s)	Year	Journal	Vol-ume	Issue/ No.	Pages	
204	2016 threats predictions	McAfee Labs & Intel	2016	online				
205	Data breach digest.	Verizon	2016	online				
206	CIS critical security controls	Center for Internet Security (CIS)	2016	online				
207	2016 data breach investigations report: 89% of breaches had a financial or espionage motive,	Verizon	2016	online				
208	Global cyber insurance update: expanding threats amplify underwriting Opportunity, Loss Potential	Fitch Ratings	2016	online				
209	CRO Forum concept paper on a proposed categorisation methodology for cyber risk	CRO Forum	2016	online				
210	Pool Re should 'evolve' to cover cyber attacks and pandemics	Ralph	2016	online				
211	Cyber and beyond: Insurance and risk in a digitally interconnected world	IBM	2016	online				

	URL	Author / publication	Academia discipline	Methodology	Risk Management	Our Keywords	Keywords from the paper
	http://www.mcafee.com/tw/resources/reports/rp-threats-predictions-2016.pdf	Industry	IT	Qualitative	Risk Management (broad sense)		
	http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf	Industry	IT	Qualitative	Risk Identification	Data Collection	
	https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf	Industry	Politics	Qualitative	Risk Management (Mitigation / Insurance)	IT Security, Self Protection	
	http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016	Industry	Finance / Insurance / RM	Qualitative	Risk Assessment	Data Collection	
	https://www.fitchratings.com/site/pressrelease?id=1001233	Industry	Management	Qualitative	Risk Assessment	Rating	
		Industry	Finance / Insurance / RM	Qualitative	Risk Identification	Risk Taxonomy	
	http://www.ft.com/cms/s/0/0d8c-7b5c-d734-11e5-8887-98e7feb46f27.html#axzz4CDXs8hQY	Industry	Finance / Insurance / RM	Qualitative	Risk Management (Mitigation / Insurance)	Insurability, Cyber Insurance, Underwriting Cyber Risk, Cyber Insurance	
	https://www.all-about-security.de/fileadmin/micropages/Studien/Cyber_and_beyond_-_Insurance_and_risk_in_a_digitally_interconnected_world.PDF	Industry	Finance / Insurance / RM	Data collection	Risk Management (broad sense)	Survey, Cyber Insurance, Data Collection	

Appendix D: Definitions of Cyber Risk

Source	Definition
Mukhopadhyay *et al*. (2005, 2013)	Risk involved with malicious electronic events that cause disruption of business and monetary loss.
Böhme and Kataria (2006)	Breach or failure of information systems.
Cebula and Young (2010)	Operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems.
Kshetri (2010)	A cybercrime is defined as a criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules, or regulations.
Ögüt *et al*. (2011)	Information security risk.
The UK Cyber Security Strategy (2011)	Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our businesses, infrastructure and services.
World Economic Forum (2012)	'Cyber risks' are defined as the combination of the probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation.
World Economic Forum (2012)	'Cyber' refers to the interdependent network of information technology infrastructures, and includes technology 'tools' such as the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.
Hua and Bapna (2013)	Cyber terrorism: Attacks implemented by cyber terrorists via information systems to (1) significantly interfere with the political, social or economic functioning of a critically important group or organisation of a nation, or (2) induce physical violence and/or create panic.
National Association of Insurance Commissioners (2013)	Defines cyber by providing typical examples: Identity theft, damage to the firm's reputation, disclosure of sensitive information and business interruption.
National Institute of Standards and Technology (NIST, 2013)	Defines cyber space as 'a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.'
Tallinn Manual (Schmitt, 2013)	Cyberspace: The environment formed by physical and non-physical components, characterised by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks.
Willis (2013)	Cyber risk can be defined as the risk connected to activity online, Internet trading, electronic systems and technological networks, as well as storage of personal data.
Swiss Re (2014)	Any risk emanating from the use of electronic data and their transmission. This encompasses physical damage caused by cyber-attacks, loss or corruption of data and its financial consequences, fraud committed by misuse of data, as well as any liability arising from a failure to maintain the availability, integrity, and confidentiality of electronically stored information—be it related to individuals, companies, or governments. In this context, cyber risk insurance addresses the first and third party risks associated with e-business, the Internet, networks and informational assets.
CRO Forum (2014)	Any risks that emanate from the use of electronic data and their transmission, including technology tools such as the Internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or governments.

Source	Definition
Institute of Risk Management (2014)	Any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.
Refsdal, Solhaug, and Stølen (2015)	Definition consisting of three elements: -A cyber-risk is a risk that is caused by a cyber-threat -A cyber-threat is a threat that exploits a cyberspace -Cyberspace is a collection of interconnected computerised networks, including services, computer systems, embedded processors, and controllers, as well as information in storage or transit.
Lloyd's (2015)	Losses relating to damage to, or loss of information from, IT systems and networks.
Lloyd's (2015a)	Definition of Cyber-Attack: exposures arising from a malicious electronic act which for the purpose of this bulletin we label as 'cyber-attack'. Cyber-attack is therefore the proximate cause of loss, although the consequences may include property damage, bodily injury, financial loss or other forms of damage.
CRO Forum (2016)	Cyber risk [is] defined as the risk of doing business in the cyber environment. The definition of cyber risk covers: • Any risks emanating from the use of electronic data and their transmission, including technology tools such as the Internet and telecommunications networks. • physical damage that can be caused by cyber attacks. • fraud committed by misuse of data. • any liability arising from data use, storage and transfer, and • the availability, integrity and confidentiality of electronic information be it related to individuals, companies or governments.

Based on a data set of 211 papers, this report provides an overview of the main research topics in the emerging fields of cyber risk and cyber risk insurance. The results illustrate the immense difficulties in insuring cyber risk, especially due to a lack of data and modelling approaches, the risk of change and incalculable accumulation risks. We discuss various ways to overcome these insurability limitations such as mandatory reporting requirements, pooling of data or public–private partnerships with the government covering parts of the risk.

The Geneva Association—'International Association for the Study of Insurance Economics'
Talstrasse 70, CH-8001 Zurich | Tel: +41 44 200 49 00 | Fax: +41 44 200 49 99

secretariat@genevaassociation.org