TEN KEY QUESTIONS ON CYBER RISK AND CYBER RISK INSURANCE—REPORT SUMMARY

THE GENEVA ASSOCIATION

This is a short summary of the first report from The Geneva Association's Cyber and Innovation research programme, Ten Key Questions on Cyber Risk and Cyber Risk Insurance. *The report 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 cyber risk and the cyber insurance market.*

Using a database of 211 studies, articles and working papers this report provides insurance practitioners and academics with a high-level overview of the insights from, and direction of, current research in cyber risk and cyber risk insurance. The focus of the research analysed is on the business and economics literature in the risk and insurance domain. In order to provide a structured discussion of the relevant literature, the analysis is structured around **three research clusters** and **10 key questions** (see Figure 1).

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

SUMMARY OF EXISTING KNOWLEDGE ON CYBER RISK AND CYBER INSURANCE

1. What is cyber risk? Definition and categorisation.
2. What are the costs and detrimental effects caused by cyber risk?
3. Where do we find data on cyber risk?
4. How can we model cyber risks?
5. Micro perspective: How should cyber risk management be organised?
6. Macro perspective: Is cyber risk a threat to the global economy and society?
7. Cyber insurance market: What is the status quo and what are the main insurability challenges?

DERIVATION OF POTENTIAL FUTURE WORK (PRACTICAL PERSPECTIVE)

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

DERIVATION OF POTENTIAL FUTURE RESEARCH (ACADEMIC PERSPECTIVE)

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

1 What is cyber risk? Definition and categorisation

- Cyber risk is 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 approaches, and risk of change.

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

- The enormous global costs estimates (up to a 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 (Biener *et al*. (2015).

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 scenario analyses for measurement and management of accumulation risk, analyse whether insurance companies can become a systemic risk due to cyber insurance, become part of the global dialogue with stakeholders.

WHAT IS CYBER RISK? *(extract, see report Foreword)*

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. This data is 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 security, integrity and failure risks. 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.

CYBER CRIME COST ESTIMATES *(extract, see report p. 14)*

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.

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

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).

However, they also point out 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) also 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 (see report p. 15).

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 examined in the paper 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 can negatively affect a company's stock price,** mainly due to reputational damage.

HOW SHOULD CYBER RISK MANAGEMENT BE ORGANISED? *(extract, see report p. 23)*

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. 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 (157 USD per record vs 236 USD per record for firms without strategic security leadership (Shackelford, 2012)).

WHAT SHOULD THE INSURANCE INDUSTRY DO TO PREVENT CYBER RISKS AND TO SUPPORT CYBER INSURANCE? *(extract, see report p. 33)*

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 stakeholders to collect and spread 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**.

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 *et al*(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.

WHAT SHOULD THE GOVERNMENT DO TO PREVENT CYBER RISKS AND TO SUPPORT CYBER INSURANCE? *(extract, see report p. 35)*

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.

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. The report does 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.

REFERENCES

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.

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.

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.

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.

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

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.

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

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

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

This paper is a summary of a report which is available, including a list of the 211 sources, on The Geneva Association website at this link: https://goo.gl/UUFZDB