NEWSLETTER
INSURANCE AND FINANCE

THE GENEVA ASSOCIATION

No. 14, August 2014

Insurability of Cyber Risk[1]

By Christian Biener, Martin Eling and Jan Hendrik Wirfs[+]

Introduction

Every reported incident of data breach or system failure resulting in high financial or reputational loss increases decision-maker awareness that current insurance policies do not adequately cover cyber risks. There are many examples of the high economic and social relevance of cyber risk such as the recent NSA, Sony, or LGT data breaches. Recently, the G20 group denoted cyber attacks as a threat to the global economy—an assessment that is not surprising considering that expected annual losses from cyber risk are estimated between US$300bn and US$1tn,[2] whereas the respective 10-year average for catastrophic losses is only US$200bn.[3] Insurance is seen as one possibility for managing cyber risk exposure. The market, however, lags behind the expectations for this potentially huge new line of business with penetration levels estimated between 6 per cent and 10 per cent of companies.[4] In our analysis, we discuss the adequacy of insurance solutions to manage cyber risk.

Definition of cyber risk

The term "cyber risk" refers to a multitude of different sources of risk affecting the information and technology assets of a firm. The definition of cyber risk we employ here is a broad one and is based on how regulators of insurance and financial markets categorise cyber risk—that is, as operational risk. However, we focus on operational cyber risk here, referring to those operational risks relevant for information and technology assets. We thus define cyber risk as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems".[5] Following the operational risk frameworks in Basel II and Solvency II, we categorise cyber risk into four classes: (1) actions of people (e.g. inadvertent loss of data by employee), (2) systems and technology failures (e.g. malfunction of hardware), (3) failed internal processes (e.g. insufficiently defined responsibilities), and (4) external events (e.g. fire).

Market overview

Commercial property and liability insurance is available in most insurance markets worldwide. However, property policies typically only cover damage to physical assets such as production facilities and exclude cyber risk, as also is the case with liability policies in general. In response to this setting, a specialised market providing coverage for cyber risks has emerged in recent years, most prominently in the United States.

As yet, however, market coverage is relatively low. Moreover, outside the United States, insurance coverage for cyber risk is not well known and not much used. In Europe, for example, about 25 per cent of corporations are not even aware that this type of insurance exists and only 10 per cent have purchased cyber risk coverage.[6] Figures for the United States show a similarly low average level of coverage of about 6 per cent, but large variations between

[1] This is the abridged version of the article to appear in *The Geneva Papers on Risk and Insurance—Issues and Practice,* Vol. 40, No. 1, 2015.
[+] Institute of Insurance Economics, University of St. Gallen, Switzerland.
[2] See McAfee (2013).
[3] See Munich Re (2014).
[4] See Willis (2013a, b), for the United States, and Marsh (2013), for Europe.
[5] See Cebula and Young (2010).
[6] See Marsh (2013).

industries among the Fortune 1000 companies.[7] According to Betterley, current annual gross premiums for cyber insurance in the United States are US$1.3bn and growing 10–25 per cent on average per year.[8] Continental Europe is estimated to generate premiums of only around US$192mn, but this figure is expected to reach US$1.1bn in 2018.[9]

Methodology and results

In our paper we discuss the insurability of cyber risk along the lines of a set of common criteria to shed light on the causes of lacking cyber insurance market development. Baruch Berliner[10] introduced a simple, yet stringent and comprehensive, approach for differentiating between insurable and uninsurable risks. This approach, which is based on nine insurability criteria, is frequently used to analyse insurance markets. The criteria are categorised into three broad groups that classify risks in terms of actuarial, market, and societal conditions. We analyse each criterion, taking into account the findings from previous literature. In addition, for the actuarial criteria we extract cyber risk loss data from an operational risk database and analyse their statistical properties. In the following we list the main problems in insuring cyber risk and summarise the most interesting findings.

- **Development of frequency and severity of losses:** for the development of cyber risks over time we find the number of incidents before the year 2000 to be relatively small, which is not much of a surprise since digital economic values were still relatively limited. After that point, however, the number of incidents continuously increased and, in the last years, accounts for a substantial part of all operational risk incidents. These findings emphasise the increasing economic importance of cyber risk in recent years. One interesting observation, however, is that the average loss decreased over the last years, which indicates an increasing use of self-protective measures that reduce losses in the event of a cyber attack.

- **Risk pooling:** correlations among cyber risks can be relatively high as compared to other risks. In addition to the commonly cited small size of current cyber risk pools efficient risk pooling and diversification is problematic and hardly achieved.[11] The development of a viable cyber insurance market could thus benefit from increasing reinsurance capacity to better spread the exposure.

- **Scarcity of data:** a principal problem in insuring cyber risks is the scarcity of data and lack of understanding of this new type of very dynamic risk.[12] Insurers react to the high level of uncertainty by setting high deductibles and low maximum coverage that result in insurance policies that are of little value to many risk managers.

- **Risk of change:** dynamic changes of cyber exposures are often drastic and fast. Not only technical aspects of progress in hardware and software as well as the use of novel networks threaten stable loss estimates, the sphere of data and systems security and integrity also is prone to a significant degree of regulation that is adapted over time. An analysis of historical cyber risk data thus could be misleading if the nature of the underlying risk has undergone substantive change.

- **Information asymmetries:** moral hazard and adverse selection are often viewed as primary impediments to market development. The complex interrelations of modern information systems result in significant vulnerability to cyber risk even though single firms invest in self-protective cyber risk measures. The interrelated nature of information systems also makes it difficult to discover, much less prove, sources of losses and identity of perpetrators, which potentially increases a firms' reluctance to invest in self-protective measures.[13] In the extant cyber insurance literature, there is some evidence that firms that have experienced a

[7] See Willis (2013b).
[8] See Betterley (2013).
[9] See NAIC (2013).
[10] See Berliner (1982).
[11] See ENISA (2012).
[12] See Herath and Herath (2011), Gordon *et al.* (2003), Baer and Parkinson (2007), ENISA (2012).
[13] See Ögüt *et al.* (2011).

cyber attack are more likely to purchase insurance, resulting in adverse selection.[14] Furthermore, the lack of data on cyber losses makes it difficult to sort firms into different risk types, thus amplifying adverse selection.[9]

- **Product value:** today's cyber insurance policies contain significant exclusions such as self-inflicted losses, the access of unsecure websites that will not trigger a claim payment. At the same time we observe relatively low cover limits of about US$50mn and exclusions of many indirect costs such as reputational losses.[15] Potential policyholders thus question the value of these products.

Conclusion and recommendations

Significant economic impacts from and increasing media attention to cyber risk make managing it imperative. In this context cyber insurance has two virtues. One is that insurance coverage puts a price tag on cyber risk and thus creates incentives for risk-appropriate behaviour. The other is that simply by applying for cyber insurance, companies become more aware of and self-protective against this threat.

However, a number of problems with the insurability of cyber risk impede the market development. The main difficulties involve randomness of loss occurrence, information asymmetries, and cover limits. However, we are able to conclude on a positive note. With increasing market development, the insurance risk pools will become larger and more data will be available. In addition, we see room for improvement in systematic data collection. For instance, insurers could either combine resources and exchange data on a multilateral basis as is done, e.g., with operational risks in banking or alternatively regulators could provide a common platform for data sharing. The rate advisory organisations that exist, for example, in the form of the Insurance Services Organization (ISO) in the United States could provide a starting template. Government involvement may even be more feasible in the case of cyber risk for several reasons. One is the infancy of the industry that impedes the development of an independent organisation for this function. A second relates to the fact that governments can require data reporting whereas independent insurers cannot. A third reason is that government schemes should be more closely aligned with public interests than would be an independent entity. In addition, regular industry surveys may capture the dynamic changes affecting the cyber insurance market and provide guidance.

A number of new competitors have entered the market in recent years and more are planning to do so. This will increase insurance capacity and market competition and keep prices down. This is also a favourable development in the context of the criticised lack of sufficient reinsurance capacity. In light of our discussion in this paper, it would seem important to establish minimum standards on coverage limits and pre-coverage risk assessment as well as clear-cut definitions of cyber risk, all of which will reduce, if not eliminate, some of the problems of insuring cyber risk. Indeed, the consulting and risk assessment services of insurance companies prior to offering cyber insurance coverage seem to be a central driver of product value, thus increasing demand.

References

Baer, W. S. and Parkinson, A. (2007). "Cyberinsurance in IT Security Management", *IEEE Security and Privacy* 5(3): 50–56.

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

Betterley, R. (2013). "Cyber/Privacy Insurance Market Survey 2013: Carriers Deepen Their Risk Management Services Benefits—Insureds Grow Increasingly Concerned with Coverage Limitations, http://betterley.com/samples/cpims13_nt.pdf, last accessed: 16 December 2013.

Cebula, J. J. and Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks,* Technical Note CMU/SEI-2010-TN-028, CERT Carnegie Mellon University.

Chabrow, E. (2012). "10 Concerns When Buying Cyber Insurance", last accessed: 18 January 2014.

ENISA (2012). "Incentives and Barriers of the Cyber Insurance Market in Europe", last accessed: 18 January 2014.

Gatzlaff, K. and McCollough, K. A. (2012). "Implications of Privacy Breaches for Insurers", *Journal of Insurance Regulation* 31: 195–214.

Gordon, L. A., Loeb, M. P. and Sohail, T. (2003). "A Framework for Using Insurance for Cyber-Risk Management", *Communications of the ACM* 44(9): 70–75.

[14] See Shackelford (2012).

[15] See Mukhopadhyay *et al.* (2005), Gatzlaff and McCullough (2012).

Haas, A. and Hofmann, A. (2013). *Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit,* FZID Discussion Paper, No. 74-2013.

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.

Marsh (2013). *Cyber Risk Survey 2013,* last accessed: 16 December 2013.

Mukhopadhyay, A., Saha, D., Mahanti, A. and Chakrabarti, B. B. (2005). "Insurance for Cyber-Risk: A Utility Model", *Decision* 32(1): 153–169.

McAfee (2013). *The Economic Impact of Cybercrime and Cyber Espionage*.

Munich Re (2013) *2012 Natural Catastrophe Year in Review*.

Munich Re (2014) *2013 Natural Catastrophe Year in Review*.

National Association of Insurance Commissioners (NAIC) (2013), "Cyber Risk," http://www.naic.org/cipr_topics/topic_cyber_risk.htm, last accessed: 7 December 2013.

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.

Shackelford, S. J. (2012), "Should Your Firm Invest in Cyber Risk Insurance?" *Business Horizon* 55: 349–356.

Willis (2013a), "Willis Fortune 500 Cyber Disclosure Report," http://blog.willis.com/downloads/cyber-disclosure-fortune-500, last accessed: 16 December 2013.

Willis (2013b), "Willis Fortune 1000 Cyber Disclosure Report," http://blog.willis.com/downloads/cyber-disclosure-fortune-1000-2013, last accessed: 16 December 2013.