Europe Economics

Cyber Risk Pool

21 February 2017

Europe Economics
Chancery House
53-64 Chancery Lane
London WC2A 1QU

Tel: (+44) (0) 20 7831 4717
Fax: (+44) (0) 20 7831 4515

www.europe-economics.com

Cyber Risk Pool

Introduction

The market for cyber risk insurance has grown exponentially over the recent years. In the US it was estimated to be worth $2 billion in 2015 and forecasted to reach the $20 billion bar within a decade.[1] By comparison, the cyber liability insurance market in Europe is considerably smaller in size. In April 2016, however, the European Council passed the General Data Protection Regulation, which is scheduled to go into effect in 2018.[2] The regulation is expected to spur demand for cyber risk insurance.

In light of the above developments, criticism and concerns have arisen regarding the extent of the industry's ability to absorb cyber risk. In particular, the capacity[3] offered for most risks is too low to provide adequate protection for potential billion-dollar losses due to cyber breaches.[4] At the same time, rating agencies are warning insurers that the accumulation of cyber risk may negatively affect their ratings.

A possible solution that has been proposed to address concerns of this sort is the formation of a cyber liability insurance pool.[5] This mechanism could result in greater capacity and less risk absorbed by individual insurers. Accordingly, the purpose of this file note is to:

- illustrate current challenges in the cyber risk insurance market;
- present the concept of a cyber risk pool;
- illustrate its inherent advantages and disadvantages; and
- discuss potential implications of a withdrawal of the Insurance Block Exemption Regulation.

Challenges within the current market for cyber risk insurance

The cyber liability insurance market is characterised by several challenges faced by policyholders and insurers alike.[6] These include:

- Lack of standardized policy forms — there are few standard policy forms being used by insurers offering cyber risk coverage. As a result, it can be difficult for policyholders to compare policies from competing markets when purchasing cyber insurance and understand which risks are indeed covered.
- Changes in the number of firms offering cyber risk coverage — there is no guarantee that an insurer currently offering cyber risk insurance will continue to do so in the long-term, thus hindering the stability in policyholder-insurer relationships.

---

1 See http://www.securityweek.com/cyber-insurance-market-top-14-billion-2022-report.

2 See http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

3 The term capacity relates to the maximum exposure which an insurer is permitted to underwrite or considers that it can prudently accept given its capital resources, risk appetite and reinsurance cover. In the context of the market as a whole, capacity refers to the collective ability of the insurers to accept risks of a given type.

4 Typical policy limits for large policies vary between $100 million and $200 million.

5 For more information on cooperation arrangements between insurance and reinsurance undertakings see Europe Economics's study for the European Commission (2017) "Different forms of cooperation between insurance companies and their respective impact on competition: Studies on issues pertaining to the insurance production process with regard to the application of the Insurance Bock Exemption Regulation (IBER)".

6 See Biener, C., Eling, M. and Wirfs, J.H. (2015) "Insurability of cyber risk: An empirical analysis". University of St. Gallen Institute of Insurance Economics. Working Papers on Risk Management and Insurance No. 151.

- Evolving nature of cyber breaches — the types of cyber breaches seem to be heterogeneous and evolving.[7] It is therefore likely that current practices will be replaced in the future by more inventive and currently unanticipated tactics.
- Exposure changes and varying coverage — as the types of breaches change so do the exposures of policyholders.[8] In this sense, disputes over coverage may still arise in response to unexpected claims or divergent legal interpretations of a given policy.
- Correlations of cyber risks — the independence condition is an important prerequisite to insuring any type of risk as the larger the number of mutually independent risks within an insurance portfolio (or pool) the more likely it is that average aggregate losses correspond to expected losses, thus decreasing insurers' safety loadings. However, this condition may not be satisfied in cyber insurance as risks may be correlated.
- Information asymmetry — moral hazard considerations manifest due to the possibility of a coordination problem as investments in cyber security generate positive externalities. Thus, the utility of cyber security investments by one firm depends on the cyber security investments by all other firms. Moreover, there is evidence that firms that have experienced cyber-attacks are more likely to purchase insurance, thus resulting in adverse selection.
- Inaccurate product pricing and loss projections — the lack of sufficient data is crucial in this respect. Credible data are of the upmost importance in order to calibrate model assumptions and estimate expected future losses. In the absence of such data, projections could be materially biased.

Overall, these challenges are capable of preventing insurers from offering cyber risk insurance. They may also impose barriers to consumers seeking cyber risk coverage as policy forms and coverage options may be too difficult to navigate.

What is an insurance pool?

It is common for unconventional risks to be covered by cooperation schemes, where multiple insurers devote capital and know-how through risk-sharing and/or information-sharing agreements.[9] More specifically, pools are arrangements comprising multiple insurance undertakings and set up to cover risks pertaining to specific risk categories (e.g. nuclear pools, terrorism pools, natural catastrophe pools). For such risks, it is perceived that a single insurer and delegated underwriting procedures in the open market would fail to provide capacity. This is to a large extent due to:

- The losses arising in the event the risk materialises being too large for any single company to be able to absorb on its own ("capacity constraint").
- The limited understanding (e.g. due to lack of historical data) of the implications of the risk and/or of its probability of occurring ("assessment constraint").[10]

As a result, cooperative insurance schemes, or pools, tend to cover such risks. Accordingly, pools historically have been a mechanism employed to provide greater insurance capacity for unconventional or emerging risks, thereby stabilising the market. There have been, for instance, in the past numerous natural catastrophe pools

[7] These include e.g. hacking, phishing, cyber extortion, and data ransom.

[8] For instance, a fridge, previously not thought to have a cyber exposure, will soon be "online" in the Internet of Things and could be the target of a cyber-attack.

[9] For instance, current examples of insurance pools include aviation pools and nuclear risk pools which were formed in the early days of flight, and nuclear technology respectively, and still exist today.

[10] See e.g. Europe Economics's study for the European Commission (2017) "Different forms of cooperation between insurance companies and their respective impact on competition: Studies on issues pertaining to the insurance production process with regard to the application of the Insurance Bock Exemption Regulation (IBER)", Jaffee, D. and Russell, T. (1996) "Catastrophe insurance, capital markets and uninsurable risks" The Wharton School of the University of Pennsylvania Working Paper 96-12, Berliner, B. (1985) "Large risks and limits of insurability" The Geneva Papers on Risk and Insurance, Vol 10, p.313-329 and. Ibragimov, R. and Walden, J. (2007) "The limits of diversification when losses may be large" Journal of Banking and Finance, Vol 31, No 8.

and programs that were established in the aftermath of an extreme event (e.g. a flood or an earthquake). As market demand drives the formation of these pools, more pools are formed (e.g. by pool managers or participating companies who decide to leave and form new pools) leading to greater competition and greater quality of services offered (e.g. in terms of claims handling).

How would a cyber risk pool operate?

In its simplest form, a cyber risk coinsurance pool could operate on a voluntary basis, sponsored by insurance companies or other financial entities, each with assumed shares. In particular, there could exist a lead insurer (with the highest share in terms of risks/claims shared and return) who sets the terms and conditions for participation in the pool. Potential followers obtain the terms and conditions from the lead insurer and decide whether to participate, and, if so, for what percentage of the risks/claims shared. Participating followers can agree to adopt the premium and conditions of the lead insurer and negotiate only with regards to the quota.

Alternatively, followers can perform their own premium calculation, although the frequency of such arrangements is limited given the inherent pricing difficulties of the risk covered. Moreover, limits on membership could be imposed based on financial strength.

The time frame for the existence of the pool could be limited — perhaps more of a tool to help develop the early market, stabilise it and allow it to grow. As seen above, additional cooperative arrangements may manifest once an initial pool has been formed. Such formations can also be instigated by insurance brokers (i.e. broker-led pools).[11]

Advantages inherent in a cyber risk pool:

In principle, a cyber risk pool would allow the industry to offer the necessary coverage needed, while also allowing the accumulation and sharing of information on cyber risk (e.g. event occurrence frequency and loss data). Therefore, by forming such an arrangement, insurers and policyholders could benefit from:

- Broader participation and capacity — smaller insurance companies looking to expand their business could participate in a cyber pool. This would allow them to enter the market in accordance to their risk appetite. Capital could also be provided by other financial entities seeking to diversify their portfolios.
- Sharing of information regarding risks — information sharing between pool members and policyholders can assist address new types of cyber threats, thus limiting the spread of a potential problem as a result of shorter reaction times.
- Standardisation of application process — a standardized application could lead to greater efficiency in the underwriting process and to more customers securing coverage.
- Uniformity of policy coverage — standardised applications and policy forms could lower the existing ambiguity over the precise nature of the risks covered, thus also facilitating comparisons.
- Pool member protection — a larger pool is likely to result in greater business volume and, hence, greater leverage for the potential purchase of reinsurance.

Disadvantages inherent in a cyber risk pool

Despite the aforementioned benefits there are several drawbacks inherent in the formation of a cyber risk pool. More specifically:

[11] See Europe Economics's study for the European Commission (2017) "Different forms of cooperation between insurance companies and their respective impact on competition: Studies on issues pertaining to the insurance production process with regard to the application of the Insurance Bock Exemption Regulation (IBER)".

- Limited competition — having several large pools in the market limits the number of competitors, at least in the short-term, as competing insurers would need to either join an existing pool or form their own and be lead insurers. The latter option, however, may not be feasible due to capacity or assessment constraints.
- Limited innovation —the presence of pools could inhibit the growth of custom polices that could address perils faced by a small number of potential policyholders. Ad-hoc coinsurance agreements set up by brokers, however, may offer a solution.[12]
- Lack of exit strategy — the dissolution of pools can sometimes result in frictions and costly litigation.

The Insurance Block Exemption Regulation (IBER)

The IBER[13] exempts certain types of information exchanges and 'pooling' agreements between insurers from the general EU competition law prohibition on anti-competitive agreements. More specifically, the IBER exemptions relate to:

- the exchange and/or aggregation of data in statistics and studies; and
- the joint insurance and/or reinsurance of risks in pools.

The Commission reached the provisional conclusion in March 2016 that it would not renew the IBER when current legislation expires.[14] This outcome followed a review in 2010 whose main findings indicated that two out of the initial four exemptions were no longer needed.

It needs to be mentioned, however, that the expiry does not mean that such cooperative forms will become illegal. Rather, similar to all other companies, insurance undertakings operating in the EU, will need to assess their cooperation in the market context to see whether it is in line with antitrust rules.

Conclusion

Faced with an increasing need for cyber risk coverage the insurance market is racing to meet the demand. However, the ability of insurers to cover such risks on a stand-alone basis may be limited and attempts to do so may result in excessive losses and/or credit rating downgrades.

The formation of a cyber risk pool could thus be the first step towards the establishment of a well-functioning cyber liability insurance market in the EU. The likely non-renewal of the IBER on March 2017, while a considerable development, is not expected to impede the ability of insurers to form such cooperative arrangements and allow the market to stabilise and grow. As cyber risks work their way up on the corporate agenda, it becomes more likely that a cyber risk pool will be instigated in the EU.

[12] See Europe Economics' study for the European Commission (2017) "Different forms of cooperation between insurance companies and their respective impact on competition: Studies on issues pertaining to the insurance production process with regard to the application of the Insurance Bock Exemption Regulation (IBER)".

[13] See http://www.insuranceeurope.eu/insurance-block-exemption-regulation.

[14] See http://ec.europa.eu/competition/sectors/financial_services/iber_swd_en.pdf.