DOI: 10.20472/EFC.2018.010.034

GRZEGORZ STRUPCZEWSKI

Cracow University of Economics, Poland

CURRENT STATE OF THE CYBER INSURANCE MARKET

Abstract:

The aim of the paper is to present the current state of the cyber insurance market. Based on recent industry reports, we identify its opportunities and threats, and discuss the most important challenges that have to be overcome by the insurance industry. The role of cyber risk reinsurance in providing capacity for insurance carriers is also shown. Finally, we try to identify current trends in demand for cyber coverage and verify if all needs of cyber insurance buyers are satisfied. In order to attract more cyber insurance customers, insurers should at least: clarify the language and the scope of cyber insurance policy, expand the advantages of cyber policy beyond simple risk transfer, develop personal cyber insurance offer.

Keywords:

cyber insurance, cyber risk, cyber reinsurance, insurance market

JEL Classification: G22, K13

1 Introduction

Cyber risk is a growing global threat. While digitization is revolutionizing business models and transforming daily lives, it is also making the global economy more vulnerable to cyber-attacks (Lloyd's 2017). The significance of cybersecurity was reflected in the World Economic Forum's 2018 Global Risks Report, which places cyber-attacks and massive data fraud among the year's top five risks (WEF 2018). It's worth to mention that for the first time two technological risks have been in the top five. Cyber risk can be defined as operational risk to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems (Cebula and Young 2010).

Digital vulnerability is driven by six trends that lead to risk aggregation. These trends are (Lloyds 2017): 1) increase in volume of software developers (risk of unintentional human errors), 2) growing number of new software, 3) open source software (potential errors in primary code), 4) using old software (it's more vulnerable than newer alternatives), 5) multi-layered software, 6) automatically generated software (more vulnerable to malicious modification).

As the cyber threat increases so too does the demand for cyber insurance. Cyber insurance is the fastest growing line of business in the insurance industry (Lloyd's 2017). Cyber insurance can fulfill a key role in the economics of cybersecurity. On one hand, by keeping the risk manageable for the insured companies by transferring it to the insurance provider, while at the same time providing incentives for improving security, requiring certain minimum protection, and thereby reducing overall risk. Unfortunately, the cyber insurance market hasn't yet developed fully, because it has to overcome several major obstacles and challenges.

The aim of the paper is the recognition of the current state of the cyber insurance market. Based on recent industry reports, we identify its opportunities and threats, and discuss the most important challenges that have to be overcome by the insurance industry. The role of cyber risk reinsurance in providing capacity for insurance carriers is also shown.

2 Methodology and data

This paper offers a better understanding of the underlying aspects of the growth of cyber insurance market. An explanatory framework based on SWOT analysis is applied to explore factors and issues that determine the current state of the cyber insurance market and its future development. It also highlights the relevance of cyber reinsurance. The methods of content analysis, compilation, induction and deduction are used.

Research findings presented in the study are derived from the analysis and review of the literature on cyber insurance, including academic papers, industry reports and insurance papers. The primary documents consulted are listed in References.

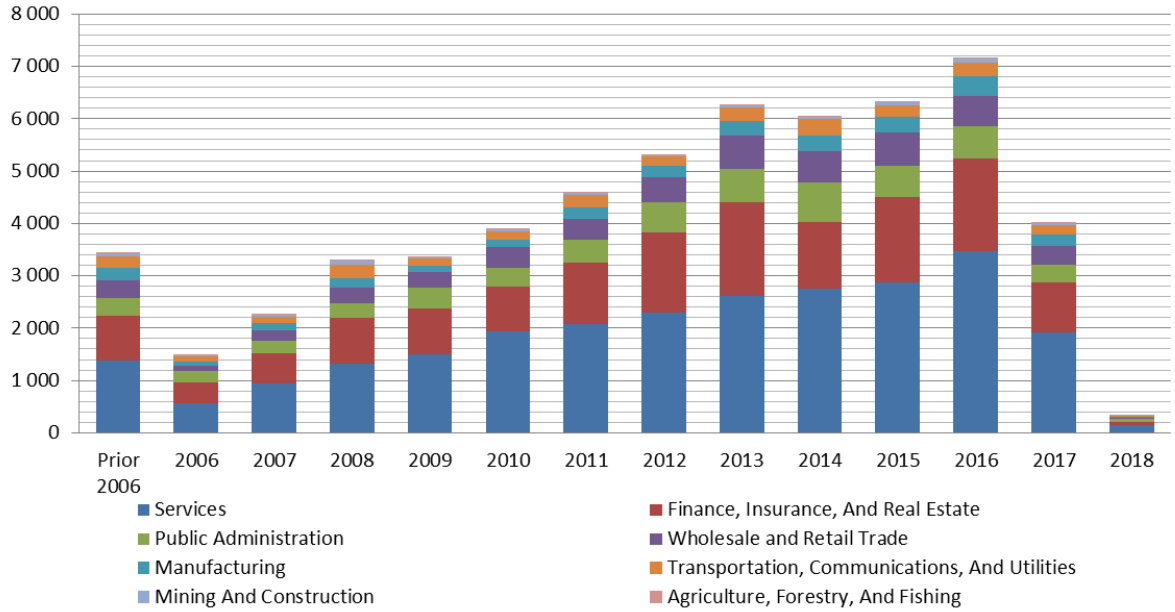
Our empirical data on cyber risk come from the Advisen Cyber Loss (ACL) database. It provides a historical view of 57,727 cyber events recorded worldwide, divided into 13 categories. 4,741 cases have attached dollar amounts of losses. The database was updated on 30th April 2018.

3 Results and discussion

Cyber risk landscape

The number of cyber incidents is growing steadily year by year (see Figure 1). Starting from 1.477 cyber events in 2006, the number of events reached 7.155 in 2016. So the 10-year CAGR is 17,1%. The event count in 2017 is substantially lower because the information about cyber incidents is still gathered and verified.

Figure 1 Cyber event count by industry and year of occurrence

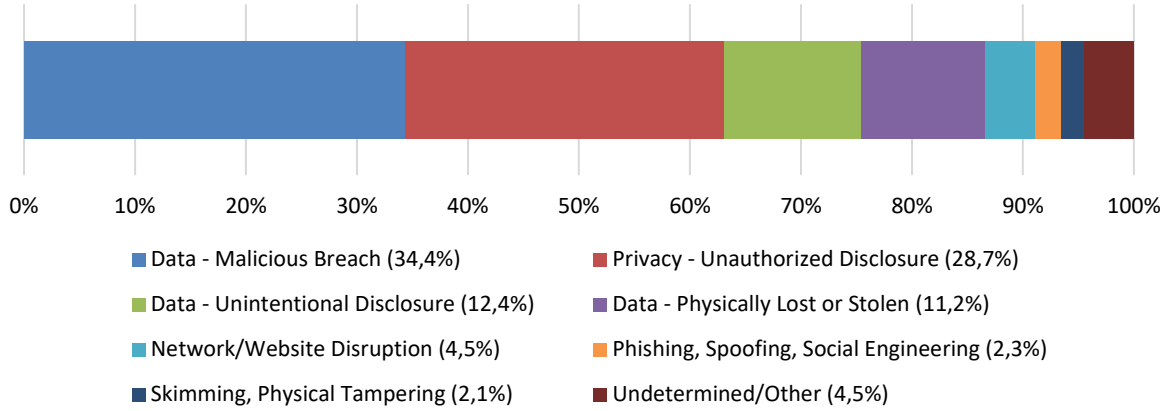


Source: own work based on the Advisen Cyber Loss database (2018).

Figure 1 provides also an insight into the structure of industries where cyber events occurred. Almost half of the total number of incidents happened in the sector of services (44,7%). Events in the financial industry represent a quarter of the entire dataset. Every tenth accident took place in public administration. The same share of cyber events was reported in wholesale and retail trade. It's worth to mention that despite the steady increase in the number of cyber incidents year by year, the industry structure of affected organizations remains stable.

Vast majority of cyber events (86,6%) is related to processing data (see Figure 2). Cyber risk manifests itself in loss, disclosure or breach of relevant data. It can result from malicious or unintentional action as well as negligence, and can be done by internal (e.g. employee, contractor, trusted third party) or external actors (e.g. hacker, former employee, criminal organization, nation state). Network and website disruptions constitute a 4,5% share of cyber events, whereas phishing and other related cyber attacks make only 2,3% of cyber loss cases.

Figure 2 Cyber event count by type



Source: own work based on the Advisen Cyber Loss database (2018).

The ACL database enables research on financial losses resulting from cyber incidents, which is unique opportunity, although the available dataset is smaller (8,2% of the entire dataset). Despite the scarcity of data, their analysis provides interesting conclusions. The total value of reported cyber losses starting from 2000 until now reached $27,5 bn (it's related to 4,741 cases). This amount includes direct economic losses, response costs, fines & penalties and litigations. In terms of financial costs, there are two major types of cyber incidents – malicious data breaches (27%) and unauthorized disclosure of personal data (27%). IT processing errors (15%) and disruptions of network or website (11%) are another types of cyber risk that represent high overall costs for enterprises. Phishing, spoofing and social engineering is the last group of cyber incidents that resulted in substantial value of financial losses (9%).

However, if we compare the above findings with the average cost[1] of particular type of cyber event, our conclusions will be different. It appears that the most costly type of cyber event is IT processing error ($78,2K). The following incidents also represent substantial average losses: phishing ($23,1K), network/website disruption ($18,7K), IT configuration errors ($16,9K). The mean cost of malicious data breach amounts "only" ca. $10.000. So we can conclude that the most severe single cyber losses have been caused by computer or network disruptions. Privacy related incidents don't transform into financial losses of an affected organization as much as it could be expected.

Indeed, as industry research shows, companies are more worried about business interruption (75%) and reputational damage (59%), than breach of customer information (55%), data or software damage (49%) and ransomware (41%) [Marsh 2018].

Cyber insurance

Cyber insurance can be defined as "protection against losses related to cyber-risks, such as data theft/loss, business interruption caused by a computer malfunction or

[1] We are aware that an arithmetic average isn't best measure of central tendency if the sample is not normally distributed, nevertheless we treat it just as an indicator.

virus, and fines or lost income because of system downtime, network intrusion and/or information security breaches" (Gartner 2015).

Insurance coverage against cyber risks is available in two forms: as cyber endorsements to classical property/liability policies, and as standalone cyber policy.

Many commercial insurance carriers offer an endorsement to cover some cyber liability and data breach exposures. Cyber endorsements are attractive to small & medium businesses because they are relatively cost efficient, and can be added to their existing policy without additional underwriting. They are usually added to policies like: commercial general liability (CGL), errors & omissions (E&O), director's & officer's (D&O), fidelity & crime, business interruption (BI), electronic equipment insurance (EEI), business owners policy (BOP), etc. However, cyber endorsements are believed to provide illusion of protection due to low loss limits and many exclusions.

Standalone cyber insurance has different sections that allow to tailor terms of coverage to the individual needs of policyholders. Insurance coverage includes both first-party losses and third-party losses resulting in legal liability. First party coverage protects against direct losses and out of pocket expenses suffered by an insured. In particular, the coverage includes: data restoration costs, direct losses of cybercrime, business interruption, cyber extortion, legal expenses, public relations expenses to manage reputational damage, forensic costs to determine the cause and extent of a breach or network event. Third party coverage is dedicated to protect against privacy liability, network security liability, media or web content liability, and privacy regulatory defense costs.

State of the cyber market

Global cyber insurance market is relatively immature. There are numerous signs that confirm this assumption: 1) lack of standardization of insurance offerings (standalone versus package policies), 2) focus on common cyber risk events that are easier to price, 3) vulnerability of new entrants to big cyber events due to imperfect risk pricing models, 4) lack of historical loss experience, 5) demand is underinformed about the benefits of cyber insurance (Geneva Association 2018).

The USA is the biggest cyber insurance market that makes 90% of the global premium written (AON 2017). The total cybersecurity insurance market in the U.S. in 2016 was $2.49 billion and ca. $3.0 billion in 2017. The share of standalone cyber policies was 52% compared to package policies representing 48% of the cyber premium (NAIC 2017; Geneva Association 2018). The second market is Europe, but European market is in its early stage. Insurers operating in Europe are repackaging their American policies and adjusting them to the needs of European customers. The premium has been low until now, but the 2018 European data protection regulation (GDPR) is expected to stimulate the market.

Cyber insurance policies sold on a standalone basis are most of the third party coverage written on a claims-made basis (approx. 98% of the cyber policies) (NAIC

2017). Claims-made policy is more convenient for insurers than occurrence based policy because it limits risk exposure by placing time limits on claim reporting.

Cyber insurance market has become profitable due to the still limited number of claims. The loss ratio for 2017 US standalone cybersecurity insurance was only 30 percent. Thus, with raising coverage limits, the market remains in soft-market phase (Geneva Association 2018; III 2018). With double-digit growth rates year-on-year, and continuous influx of new entrants, the US cyber insurance market is projected to reach $7,5 billion by the end of the decade (PWC 2015). Despite severe competition among numerous insurers, the US cyber market is dominated by three main carriers that control nearly half of the market (Geneva Association 2018).

Cyber insurance market is divided into two segments of customers: large enterprises and small/medium enterprises (SME), where the former dominates the latter. Large companies represent more mature attitude to cyber risk (large IT departments, dedicated resources to manage cyber risk, Chief Information Security Officer, understanding of cyber vulnerabilities and exposures, external IT consultants, purchased cyber insurance), whereas SMEs are not so cyber-oriented and well-developed (sale process of cyber insurance for SMEs is slow and costly, creation of cyber awareness and training on cyber risk assessment is often necessary before cyber policy can be signed) (Geneva Association 2018).

The strongest growth of premium is anticipated in Business Interruption (BI) and Contingent BI coverage (PWC 2018), but it raises questions on how to adjust a BI loss without physical damage. Despite high demand, it’s still challenging for insurance companies to price this risk. Cyber BI costs are more difficult to project because they depend on such factors as the sophistication of the attack, the organization’s business model, the level of planning and investment made before the attack, and the type of technology (Marsh 2018).

Reinsurance of cyber risk

Reinsurance plays a vital role in in enabling an insurance market to grow, particularly if insurers must cope with a new and unrecognized risk such as cyber risk. Global cyber reinsurance market is estimated to be worth $525m (Scor 2017). Most insurers (95%) buys proportional quota share reinsurance contracts, which is typical on immature markets, but due to intense competition non-proportional (Excess-of-Loss) structures are emerging (Scor 2017). The portion of retained cyber risk in XL contracts varies across insurance companies (PWC 2018).

Due to the problem with understanding and pricing cyber risk that is aggressive and fast-evolving, reinsurers remain conservative about their cyber risk exposure (in quota-share treaties the share of reinsurer is only 20-30%) (AON 2017). Consequently private reinsurance sector is capable of providing the coverage required for “everyday” risks of data breach or IT technology, but public-private partnership (for example a state reinsurance pool) would be a good alternative in providing cover for cyber terrorism or state-sponsored cyber attacks (JLT Re 2017). Alternatively, additional funds from capital markets could be acquired by issuing insurance linked securities

(ILS) in order to expand reinsurance capacity. Creation of the Global Cyber Index by PCS is the first step to developing cyber-focused ILS products (PCS 2018).

Moreover, there's also increased interest in using captives to cyber risk. Captive is a risk transfer vehicle that enables enhanced risk management, reinsurance, optimizing cost of risk and tax benefits. As more than 80% of Fortune 500 companies use captive-based solutions, it's highly possible that the same approach will be extended to cyber risk (Guardtime 2014).

Insurance protection gap

We define insurance protection gap as a difference between total economic losses and insured losses arising from a particular event. In case of cyber risk, Lloyd's (2017) estimated cyber protection gap based on analysis of two scenarios: hacktivists attack on cloud service provider resulting in business interruption, and mass cyber attack on users of popular operating system through a recently discovered exploit (so-called 'zero-day' vulnerability) – see Table 1.

Table 1 Cyber protection gap for two catastrophic scenarios

Scenario	Economic losses		Insured losses		Loss covered (%)	
	Large loss	Extreme loss	Large loss	Extreme loss	Large loss	Extreme loss
Cloud service disruption	4.60bn $	53.05bn $	0.62bn $	8.14bn %	13 %	17 %
Mass software vulnerability	9.68bn $	28.72bn $	0.76bn $	2.07bn $	7 %	7 %

Source: Lloyd's (2017).

The cloud service disruption scenario shows that the protection gap is between US$4 billion (large loss) and $45 billion (extreme loss). It means that only 13% and 17% of the losses are covered, respectively. The insurance gap in the second scenario lies between US$8.9 billion (large loss) and $26.6 billion (extreme loss). So merely 7% of economic losses would be covered.

Opportunities and barriers to growth of the cyber insurance market

The insurance protection gap can be interpreted twofold: as an opportunity to cyber insurance market growth (high unmet demand) or as a sign of serious obstacles undermining insurance offers by carriers (insufficient supply), or both. The complex issue will be examined in this section.

We present the results of our research on opportunities and barriers to growth of the cyber insurance market. We identified major trends of the market as well as its most serious challenges. We also pointed out some strategic directions that can help boost cyber insurance sales in the near future.

Main opportunities to growth of the cyber insurance market:

- Extreme cyber incidents – thanks to mandatory notification of cyber incidents and media coverage, people and businesses will become more aware of cyber

threats they are exposed to, and consequently more prone to cyber insurance purchase,

- The new EU GDPR Regulation, that will take effect from 25th May 2018, is expected to stimulate demand for cyber insurance in Europe; the same effect was observed in the US after adopting state laws requiring companies to report data breaches,
- Requirement of having cyber liability coverage set by contractors (quasi-mandatory insurance coverage),
- Growing awareness of cyber threats arising from the Internet, digitization, Internet of Things, e-banking and many other modern solutions that are developing all around.

We can see three directions of future development of the cyber insurance market:

- Clearly define which insurance policies address cyber risk, standardize and simplify cyber insurance language.
  Better clarity is needed to increase customer awareness and understanding of cyber insurance.
- Cyber insurance as a service, not just a coverage.
  Insurance companies face the unprecedented change in the insurance paradigm that requires the transformation of their business models. Due to extremely complex issue of cyber security, providing cyber insurance can't mean just simple risk transfer any longer. In the past, insurers were present only after a loss event. Now, purchase of a cyber policy should add value to an organization by offering additional services like risk consultation, risk monitoring and assessment, prevention, data breach resolution and recovery after a cyber attack. It also means close relationship with customers.
- Personal cyber insurance as the next stage in the evolution for cyber.
  Gradual increase of cyber threat awareness among individual people coupled with financial losses generated by cyber attacks on households can open a new niche on the cyber insurance market – demand driven by the need to ensure the security of human privacy, financial resources and property.

We identified critical barriers to growth of the cyber insurance market that can also be seen as challenges to solve:

- Scarcity of historical loss data.
  According to PWC (2018), average number of years of available cyber data is 7 years, only 19% of insurers have claims history of more than 10 years. Insurance carriers try to adopt claims data from other insurance lines which can be a risky approach.
- Difficulties in quantifying cyber risk.
  There is too many factors, dynamic nature of cyber risk, systemic and extreme nature of cyber risk, dealing with intelligent adversaries and intentionality which alters traditional risk modeling. Moreover, modeling typical risks from physical world differs from modeling cyber risk. The former focus on high frequency/low

impact or low frequency/high impact events whereas the latter addresses high frequency/high impact cases that can arise from interdependency and high correlation of cyber risk. In this sense we can talk about a change in insurance paradigm.

- Interdependent security.
  Many clients of an insurance company can be affected by the same attack.
- Moral hazard (reducing security investments after the purchase of cyber insurance).
- The problem of so-called ‘silent risk’.
  Silent risk arises if traditional insurance policies cover cyber risks because they neither specifically include or exclude them. Silent risk requires prudent identification, quantification and management.
- Cyber risk might be underpriced.
  Lack of confidence that cyber risk is priced adequately due to the following facts: quality and granularity of cyber data varies between insurance companies, and cyber data from the past can be irrelevant in modeling future losses. At the April 2018 reinsurance renewal, prices for cyber excess-of-loss reinsurance had fallen by between 5% and 10% because of lack of huge claims – it makes the cyber risk underpriced according to Christian Mumenthaler, the CEO of Swiss Re, the largest reinsurance company in the world (S&P Global Market Intelligence 2018).
- High and unexplored tail risk, paired with low prices of insurance policies make insurance and reinsurance business unattractive.
- Intangible assets (data, reputation, etc.).
  More and more assets of companies include intangible assets that represent high value, are of fundamental importance for running a business, and are particularly exposed to cyber risk. It rises questions: How to insure them? and How to value them?

4 Conclusions

While the cyber insurance and reinsurance space is developing, the inherent complexity and unpredictability of the exposure has made underwriting and pricing cyber risks very challenging for the industry, exacerbated by the continued and rapid evolution of the cyber risk landscape. For both insurers and reinsurers cyber is a great challenge and opportunity, offering diversification and revenue, but also potentially leading to larger losses in the future.

Once a big cyber event occurs and cyber risk awareness grows, more firms will decide to buy cyber policy. It is also probable that the government will start seeking a comprehensive solution of the problem. In order to attract more cyber insurance customers, insurers should at least: clarify the language and the scope of cyber insurance policy, expand the advantages of cyber policy beyond simple risk transfer, develop personal cyber insurance offer.

The engagement of insurance companies in all phases of the cyber risk value chain can be mutually profitable because insurers will capture more insights and knowledge from the market, offering help in cyber risk management for their customers at the same time as value added.

Acknowledgments

This research received financial support from the resources granted to the Faculty of Finance and Law of the Cracow University of Economics as part of the subsidy for the maintenance of the research potential.

References

AON (2017). *Global cyber market overview. Uncovering the hidden opportunities*. Retrieved from: http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf

Cebula, J.J., Young, L.R. (2010). *A taxonomy of operational cyber Security risks: technical Note CMU/SEI-2010-TN-028*. Software Engineering Institute, Carnegie Mellon University.

Gartner (2015). *Five Tips for Companies Considering Cyber Insurance*. March 2, Gartner Blog Network. Retrieved from: https://blogs.gartner.com/john-wheeler/five-tips-for-companies-considering-cyber-insurance/

Geneva Association (2018). *Cyber insurance as a risk mitigation strategy*. April 2018. Retrieved from: https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_insurance_as_a_risk_mitigation_strategy.pdf

Guardtime (2014). *Cyber, reinsurance, risk transfer & KSI*. Retrieved from: https://media.voog.com/0000/0036/0235/files/Guardtime%20-The%20Black%20Swan%20Event%20of%20the%20IT%20Industry.pdf

III (2018). *Cybersecurity insurance growth continues*. Insurance Information Institute, April 30. Retrieved from: http://www.iii.org/insuranceindustryblog/

JLT Re (2017). *Unlocking the potential of the cyber market*. April 2017. Retrieved from: https://www.jltre.com/our-insights/viewpoints/viewpoint-april-2017

Lloyd's (2017). *Counting the cost. Cyber exposure decoded*. Emerging Risks Report. Retrieved from: https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2017/cyence/emerging-risk-report-2017---counting-the-cost.pdf

Marsh (2018). *By the numbers: Global cyber risk perception survey*. February 2018. Retrieved from: https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Marsh%20Microsoft%20Global%20Cyber%20Risk%20Perception%20Survey%20February%202018.pdf

NAIC (2017). *Report on the Cybersecurity Insurance Coverage Supplement*. Bulletin of the National Association of Insurance Commissioners, August 6th. Retrieved from: http://www.naic.org/documents/cmte_ex_cybersecurity_tf_rpt_cyber_ins_coverage_suppliment.pdf?51

PCS (2018). *Everything you need to know about the PCS Global Cyber Index*. Property Claims Services. Retrieved from: https://www.verisk.com/siteassets/media/pcs/pcs-global-cyber-index.pdf

PWC (2015). *Insurance 2020 & beyond: Reaping the dividends of cyber resilience*. Retrieved from: https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

PWC (2018). *Are insurers adequately balancing risk & opportunity? Findings from PwC's global cyber insurance survey*. Retrieved from: https://www.pwc.com/us/en/industry/assets/pwc-cyber-insurance-survey.pdf

S&P Global Market Intelligence (2018). *Swiss Re CEO: 'It just doesn't make sense' to write more cyber insurance*. 4th April. Retrieved from: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/44121501

Scor (2017). *State of the cyber (re)insurance market*. September 2017. Retrieved from: https://www.scor.com/en/files/state-cyber-reinsurance-market

WEF (2018). *The Global Risk Report 2018. 13th Edition*. World Economic Forum, Geneva. Retrieved from: https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/the-global-risks-report-2018.pdf