THE GENEVA ASSOCIATION

Cyber Insurance as a Risk Mitigation Strategy

April 2018

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 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.

$(IC)^3$

The Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, $(IC)^3$, is headquartered in the MIT Sloan School of Management. In collaboration with other parts of MIT, $(IC)^3$ is addressing the important need to improve the cybersecurity of critical infrastructure through an interdisciplinary research approach focused on the strategic, managerial, and operational issues related to cybersecurity.

$(IC)^3$ brings together thought leaders from industry and government with MIT faculty, researchers and students, conducting research in multiple relevant areas. $(IC)^3$ conducts a variety of meetings, workshops, conferences, and educational activities, and produces research reports which can be used by its members to improve critical infrastructure cybersecurity. Please visit us at http://ic3.mit.edu

BCG Platinion

BCG Platinion, a company of The Boston Consulting Group, consists of cybersecurity experts, architects of IT solutions, implementation, and risk management experts that help achieve the right path forward for companies with complexity who seek to deliver results. BCG Platinion connects with and extends BCG's capabilities into implementation for IT, digital, cybersecurity, and risk as well as cybersecurity strategy. BCG Platinion drive projects through speedy implementation at a lower cost with swiftness and executional certainty. BCG Platinion in North America is based in New York. For more information, please visit bcgplatinion.com.

Cyber Insurance as a Risk Mitigation Strategy

List of Authors:

Michael Siegel, Principal Research Scientist, MIT Sloan School of Management and Research Director of MIT-(IC)[3]

Nadya Bartol, Associate Head of Cybersecurity Practice, BCG Platinion

Juan Jose Carrascosa Pulido, MBA Graduate Student, MIT Sloan School of Management

Stuart Madnick, Professor, MIT Sloan School of Management and Faculty Director of MIT-(IC)[3]

Michael Coden, Head of Cybersecurity Practice, BCG Platinion, and Associate Director, MIT-(IC)[3]

Mohammad Jalali, Research Scientist, MIT Sloan School of Management

Michael Bernaski, Associate Director, The Boston Consulting Group

The Geneva Association

The Geneva Association—International Association for the Study of Insurance Economics
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—Kris Tan, Shutterstock.

April 2018

Cyber Insurance as a Risk Mitigation Strategy

Contents

Acknowledgements

This paper has been prepared in collaboration with the MIT Sloan School of Management and the Boston Consulting Group. We have profited greatly from discussions with numerous academics and practitioners, and we are especially grateful to those who made themselves available for in-depth interviews:

Daljitt Barn, Global Head of Cyber, Munich Re
Maya Bundt, Head Cyber and Digital Strategy, Swiss Re
Simon Dejung, Global P&C Engineering Underwriter, SCOR
Eric Durand, Head Cyber Center of Competence, Swiss Re
Mark Dunham, Reinsurance and Exposure Manager, Aviva
Carin Gantenbein, Head Business Development and Transformation, Zurich Insurance
Tracie Grella, Global Head of Cyber Risk Insurance, AIG
David Ho, Head of Financial Institutions Financial Lines, AIG Asia Pacific
Lori Bailey, Global Head of Cyber Risk, Commercial Insurance, Zurich Insurance
Philipp Lienau, Overseer of Cyber Insurance, HDI Global SE
Gordon Payne, Director of Commercial Insurance, Intact
Chris Peters, VP & Chief Security Officer, Entergy
Marc Radice, Head of International Affairs, Zurich Insurance
Douglas Robare, Global Head of Underwriting—Financial Lines, Generali
Adam Schwarz, Director of Research and Development, Fermat Capital Management
Patrick Smolka, Head of Financial Lines, HDI Global SE
Christian Stanley, Casualty Executive Performance Management Directorate, Lloyd's of London

Additional thanks to **Mohin Khushani** (BCG), **Edwin Fawley** (MIT and Brown University) and **Daniel Hofmann** (The Geneva Association) for their support.

Foreword

Anna Maria D'Hulster

Secretary General,
The Geneva Association

While the cyber insurance market still lingers in its infancy, no one can miss its dynamics. It is the fastest growing line of business in the industry. In just a few years, cyber insurance premiums have grown to an estimated USD 2 billion in North America and USD 3 billion globally. And these volumes are expected to continue to grow. A combined assault of daily front-page news about cyberattacks, increasing government regulation and insurance industry awareness keeps raising the profile of cyber risk.

This report is the second in the research programme on Cyber and Innovation that The Geneva Association established in 2016. It intends to provide a platform for industry discussion on cyber risk and insurance and will seek to develop and inspire research and insights that support its sustainable development. The new paper analyses the state of the cyber market and the role insurers play in advancing cyber resilience. Moreover, it reviews the transformation along the value chain as insurers are moving from providing risk transfer products only to offering prevention, mitigation and resolution services.

In light of the market dynamics it should not surprise that the report raises more questions than it answered. Issues related to accumulation risk, capacity and to the broader challenges of insurability and sustainability will continue to inform our research agenda. We are looking forward to producing more building blocks in support of a viable cyber insurance market.

The paper is based on a review of the literature on cyber risk as well as interviews with brokers, customers, reinsurers, and underwriters in the U.S., Europe, and Asia. Our appreciation goes to the Massachusetts Institute of Technology and BCG Platinion for their collaboration in preparing the report.

Anna Maria D'Hulster
Secretary General of The Geneva Association

Executive summary

Cyber insurance is the fastest growing line of business in the insurance industry. A combined assault of daily front-page news items about cyberattacks, increasing government regulation and insurance industry awareness are all raising the profile of cyber risk. This is no longer just an IT-based risk but also a major business risk that is being considered at company board and ownership levels. According to surveys, 99 per cent of all boards of directors discuss cyber risk on a regular basis,[1] and 80 per cent of CEOs consider cyber risk the number one threat to business growth.[2] As more regulations are adopted, including global notification requirements such as fines and penalties, the corporate sector is looking to insurance to offer mitigation solutions that can effectively deal with this emerging risk.

Risk transfer and services

There is indeed a major opportunity for the insurance industry to help mainly corporate and commercial customers better manage and mitigate cyber risks. By doing so, insurers also tap into revenue streams in an entirely new specialised line of business:

1. Providing cyber risk transfer in the form of cyber insurance policies; and

2. Providing cyberattack prevention and mitigation services to help companies reduce the occurrences and the impact of a cyberattack.

In just a few years, cyber insurance premiums have grown to an estimated USD 2 billion in North America and USD 3 billion globally. These volumes are expected to continue to grow. Insurers provide a much-needed service for customers in terms of cyber risk prevention, mitigation and loss compensation.

Cybersecurity services are a new revenue stream for insurers. There are essentially two phases where insurers can be active:

1. **Pre-breach:** Insurers work to design appropriate cyber insurance policies for their future clients. They work with customers to better understand risks and to prevent breaches based on appropriate risk management frameworks. Insurers also offer services to increase cyber awareness in the company, assess clients' contingency plans, train personnel, or recommend best practices to reduce the effect and fix the breach. These services help to reduce the impact of an attack or an incident when it occurs.

2. **Post-breach:** Insurance policies provide services that evaluate the impact, investigate the attack, help implement response and recovery plans, provide forensics, public relations and communications support, notify customers, and identify appropriate mitigating actions to strengthen resilience in the future.

Services yield data which will fuel growth

The benefits of providing cybersecurity services go beyond generating an additional revenue stream and introducing an additional form of protection to customers. Insurers also collect valuable data regarding cyber risks, cyberattacks, successful mitigation strategies, and financial impact. This helps to build a critical data set for rating future customers, modelling cyber risks, and underwriting and pricing future services.

This data is crucial for fuelling the growth of cyber insurance in a large market for two reasons: first, insurers often do not have enough data to accurately price products; and second, without sufficient data about losses and claims payments, it is difficult to explain and sell a product to customers.

Hypotheses evaluated

In this paper, we analyse the state of the cyber insurance market and the role insurance can play in advancing cyber resilience. To structure our research, we formulated and tested three hypotheses:

1 BCG survey of clients (2015).
2 PwC survey of clients (2016).

1. Insurance companies operating in the cyber insurance area are experiencing a transformation along the value chain. They are moving away from only providing risk transfer products to also offering prevention, mitigation and resolution services.

2. Insurers have the unique opportunity to influence and improve cyber risk operations for their customers. The new collaborative model and the larger presence of insurers can be leveraged to create cyber risk awareness and improve coordination in customer organisations.

3. The cyber insurance market is still in its infancy and is in constant transition with potentially important tipping points.

Methodology

The authors of this report used two independent methods to research the market and to validate the results. The initial investigation included a thorough examination of existing academic research materials, and documentation from various organisations and companies in the cyber risk and insurance ecosystem. In addition to the literature review, information was gathered by conducting more than 45 interviews with underwriters, brokers, reinsurers, and customers in the U.S., Europe and Asia. The results of the literature review and interviews were then analysed by a team of cybersecurity and insurance experts at the Massachusetts Institute of Technology (MIT) and the Boston Consulting Group (BCG).

Key challenges

Throughout our research we encountered several challenges:

1. Many of the cyber risks are not yet well understood.

2. There is a prevailing concern about the potential for large accumulation and/or aggregation risk.

3. Lack of data and lack of data sharing are contributing to the uncertainties of how to develop and market insurance products, define the limits of insurability, and develop effective backstop solutions either with governments or through public-private partnerships.

4. The potential impact of multiple government regulations in multiple geographies and jurisdictions (often within the same country) adds significantly to the uncertainty.

5. The effects of technological developments are unknown. This uncertainty is compounded in at least three areas:

    a. The global trend towards digitisation in many industries introduces technologies with unknown vulnerabilities;

    b. It is unclear how long it will take to develop improved cyber security tools and how successful they will be in protecting digital industrial systems. In addition, standards of cyber governance are still underdeveloped;

    c. The development of new cyberattack tools by cybercriminals and nation states is entirely unpredictable.

6. There is a major difference in the cyber awareness and needs of large enterprises compared to small and medium-sized enterprises (SME).

7. There is confusion in the customer base as to who should evaluate and purchase cyber insurance—the Chief Information Security Officer (CISO), Chief Risk Officer (CRO), Chief Technology Officer (CTO), Chief Operating Officer (COO), Chief Executive Officer (CEO), or the Board of Directors.

Topics for future research

The authors of this paper also identified a number of future research topics, including:

- **Insurability**—Given the entirely new and still unexplored features of cyber risk which includes matters relating to randomness and attribution (are cyber

incidents regularly insured events or results of terror or war?), questions relating to insurability and the parameters to enable insurability need to be explored.

- **Accumulation risk**—The global nature of cyber risk with its many interlinkages across industries and sectors raises the issue of accumulation risk. Risk modelling in this area is still in its infancy.

- **Capacity**—Related to accumulation risk is the question whether the global (re)insurance industry can command the capital to absorb what ultimately may be a very large probable maximum loss. This also leads to the question whether governments will need to provide a backstop (similar to those in terrorism insurance) and to what extent global capital markets would be prepared to accept the securitisation of cyber risk.

- **Understanding cyber risk in terms of other insurance**—What can we gain by looking at other insurance markets and products (e.g. extreme natural catastrophe events, terrorism, war)?

- **Understanding market dynamics**—Better tracking and prediction methods are needed for cyber insurance market movements, entry and exit of players, impacts on market pricing, the impact of cyber events, metrics, and overall learning as the marketplace absorbs more information.

- **Creating an effective value chain**—Finding the right mix of services, in-house vs partnering, charging for services, required vs voluntary services are just a few of the issues in building the cyber risk service value chain.

- **Understanding the political, macro- and microeconomic impacts of cyber risk**—Many of the aspects of cyber risk are playing out in the international community in terms of politics, regulations, and trade policies. How these will impact insurers today and in the future is a very important aspect of the insurance marketplace.

Conclusion

Insurers are uniquely positioned to help their customers improve cyber awareness, and better understand and manage cyber risks. In addition to the growth of policies for cyber risk transfer, the cyber risk insurance value chain provides a range of cybersecurity services. This offering includes not only risk mitigation and protection services for customers but also valuable data for insurers regarding cyber risks, cyberattacks, successful mitigation strategies, and the financial impact of actual cyber events.

1. Introduction

Digitisation is a powerful economic and societal force shaping and improving lives and futures around the globe. Digitisation is in fact fuelling world economic growth. With digitisation comes increased impact and awareness of cyber risks. If not properly addressed, cyber risks have the potential to constrain and even reverse the forward momentum of digitisation which could adversely impact the world economy.

- While cyber insurance is frequently mentioned as an appropriate risk transfer mechanism, it is only recently that cyber insurance has become a marketable offering. Cyber insurance differs from other lines of business and introduces a number of challenges: cyber insurance can be considered both a product and a service, it can be a part of many lines of insurance or it can be offered as a stand-alone service.

- As everything is increasingly connected, cyber risk is ubiquitous and fluid, making its management difficult and dynamic.

- Cyber risk involves both tangible and intangible assets and activities—putting a value on losses involves judgment not evidenced and conventions not yet established.

- In most areas, cyber risk will continue to evolve and it will take time to 'mature' into a more stable state.

- The anonymity that the cyber space provides makes the attribution of cyber incidents difficult.

- Because it is not subject to physical world constraints, cyber risk does not conform to insurance risk models typically addressing either high severity/low frequency or low severity/high frequency events that in most cases are based on the idiosyncratic nature of the insured risk. Instead, cyber risk has the potential to be highly correlated across industries around the world, and, as a result of risk accumulation and aggregation, it can produce costly high severity/high frequency events.

The cyber insurance market is like other markets that are not yet fully developed in that (1) demand is inconsistently informed; (2) uncertainty and behavioural distortions impede decision-making; (3) common vocabularies are not broadly adopted; (4) suppliers' solutions are not standardised; (5) historical knowledge is limited; (6) industry regulators (such as the FCC in the U.S.) are unsure of their role and what to do; and (7) the ecosystem is fragmented. As a result, participants cannot appreciate the nature of the risk and the efficacy of preventive measures. Informational asymmetries create issues related to moral hazard and adverse selection.

The recent history of cyber exploits reflects a slow awakening to exposure and a surge of activity based on the latest headline event. To truly get ahead of the risk requires principled and visionary leadership, agility and collaboration.

The aim of this research is to provide insights into the cyber insurance market, identify future trends, and suggest areas for market development and improvement.

First, the report elaborates on some of the greatest challenges that insurers active in the cyber space are facing, from how to deal with accumulation risk to the sharing of incident data to improve risk modelling tools.

Second, we will review how insurance companies are transforming their offerings from strictly risk transfer products to a comprehensive series of offerings along the cyber risk value chain.

Third, we will analyse how insurers can educate customer organisations and collaborate with them so that they are better prepared to manage their risk.

Lastly, the report will reflect on the evolution and currently limited maturity of the cyber insurance market by analysing its status and proposing a market model to illustrate possible future developments.

2. Methodology

We conducted our research in three phases:

- **Phase 1: Literature review**—We conducted a thorough search and review of the published literature on 'cyber risk' and 'cyber insurance.' The list of documents includes industry reports, insurance papers and academic papers among others. The primary documents consulted are listed in the References section.

- **Phase 2: Internal knowledge**—The MIT Sloan Interdisciplinary Consortium on Improving Critical Infrastructure Cybersecurity, MIT-(IC)[3] and the Boston Consulting Group, BCG, synthesised experience and meaningful insights from extensive work done in the cyber risk sector in recent years. Their work helped identify the hypotheses and lines of work on which to focus for this research. This interaction also helped to generate the interview guidelines for the next stage of the project.

- **Phase 3: Insurance and customer interviews**—Our initial research is supported by more than 30 interviews that BCG Platinion conducted with insurers, experts and customers. Additionally, another 15 interviews were held to focus on our three leading hypotheses: (1) insurers are experiencing a transformation as they expand their services along the value chain; (2) insurers can significantly influence their customers to improve cyber awareness and remove their protection gaps; and (3) cyber insurance is still in its infancy, but the market is evolving, and its expansion is driven by regulation and cyber incidents.

3. General challenges in the cyber insurance market

From self-driving cars to smart insulin pumps, technology is constantly transforming and improving our lives; however, these technologies reveal vulnerabilities that, if exploited, could result in disaster.[3]

Imagine a case in which a hacker remotely accesses a self-driving car (an event of this nature has already occurred).[4] If a hacker were able to redirect a car to collide with a structure, the car, the structure, and everything in it could be severely damaged, people could be injured and the car manufacturer's reputation could suffer. How can we better understand this cyber event and its associated risks?

Cyber risk is defined differently depending on the perspective of those defining it. From the Chief Risk Officer Forum,[5] the definition of cyber risk covers:

- Any risk arising from the use of electronic data and its transmission, including technology tools such as the Internet and telecommunications networks.
- Physical damage that can be caused by cyberattacks.
- Fraud resulting from the misuse of data.
- Any liability related to data usage, storage and transfer.
- The availability, integrity and confidentiality of electronic information, whether related to individuals, companies, or governments.

The example of an attack on a self-driving car unequivocally fits into the above definition of cyber risk, but less clear are the insurance obligations that would come into effect following the incident. Would the car manufacturer's plant, property & equipment (PP&E) insurance cover damage to the car? Would the car insurance cover the damage to the structure and its contents? Which policy would protect damage to the car manufacturer's brand? Who would pay for the investigation? Would the answers to these and other questions be driven by legislation and regulation?

This example is not purely theoretical. Hardly a day goes by without another cyberattack mentioned in the press. For example, the price paid by Verizon in its acquisition of Yahoo! decreased by USD 350 million to USD 4.48 billion after the breaches that Yahoo! had suffered were disclosed.[6]

Insurers are responding to greater frequency and awareness to cyberattacks with the development of specific cyber risk insurance policies. In addition to traditional coverage, insurers are also providing services to enable their customers to be better prepared overall to manage cyber risks and quickly address the impacts in the aftermath of attacks or incidents. We will revisit this point later in Chapter 4: *The insurance role in cyber risk transfer*.

Despite the evolution of the cyber insurance market, customers struggle to understand their exposure and appetite for risk transfer. Cyber risk policies are technical and are complicated by the fact that they are standardised along a single offering model; some underwriters offer stand-alone policies, while others integrate cyber insurance in current offers without making any distinction. Customers and insurers are struggling with the issue of silent risk.[7] Moreover, insurance pricing and risk models continue to evolve. Additionally, many customers do not see any value in cyber insurance because they do not understand their cyber exposure. In Section 4.2: *Coordinating the cyber insurance ecosystem* we will elaborate on how insurers can help customers reduce their cyber risks to an acceptable level.

Customers are demanding more extensive coverage, and insurers are jumping into the market with new offerings to satisfy those needs. Large client companies are more mature in their thinking and have developed internal cybersecurity capabilities or have partnered with third party organisations to address their needs. However, small and medium client companies are generally more exposed as they do not have the resources to address all their cybersecurity needs. The insurance market is rapidly changing to address this range of demands. This paper will

3 https://www.weforum.org/agenda/2017/02/our-critical-infrastructure-is-more-vulnerable-than-ever-it-doesn-t-have-to-be-that-way/
4 https://www.tesla.com/autopilot
5 http://www.thecroforum.org/
6 www.bloomberg.com, 2017-02-21, Verizon said to reach deal for lowered Yahoo! price after-hacks
7 Silent cyber risk refers to cyber exposures that are not specifically included or excluded by (non-cyber) insurance policies. The silent exposures inherent in non-cyber policies can be significantly exacerbated by cyber events. It is estimated that silent risk can make up 90 per cent of total cyber exposures (see E. Kopp *et al.* (2017), Cyber Risk Market Failures and Financial Stability, IMF).

discuss cyber insurance market dynamics in Chapter 5: *The growing cyber insurance market*.

Finally, we consider some of the biggest challenges to the cyber insurance industry. The following paragraphs synthesise what has already been published in many industry reports with insights gleaned from our interviews.

3.1 The unique nature of cyber risk

Insurance companies are used to dealing with many areas of uncertainty and risk. They offer coverage for natural disasters, business interruption, and even damage from terrorist attacks; however, insurance companies are not used to dealing with many of the new incidents of cyber risk.

One way to conceptualise the implications of a cyberattack with regard to damage is to compare it with an earthquake. An earthquake can happen anywhere, anytime. It can cause property damage, personal injuries and losses, and can interrupt business operations and supply chains. A cyberattack can cause the same damage. For example, a hacker could target the control system of a pressure valve in a nuclear power plant and cause damage comparable to the earthquake and tsunami that nearly destroyed the Fukushima nuclear plant in Japan.

However, cyber incidents do not only occur with high severity, they can also occur with high frequency

In this sense, the nature of a cyber incident is different to that of a natural disaster (e.g. earthquake). Based on many years of observations and historical records, we know that natural disasters occur with a certain frequency. For example, the likelihood of having several simultaneous earthquakes around the world is very small, but cyberattacks can happen to any number of organisations simultaneously. The recent WannaCry attack exemplifies the global and spontaneous nature of a widespread cyberattack. Experiencing an attack does not necessarily prevent the same company from experiencing a second attack immediately after the first. This will depend on the speed of identification, analysis, and mitigations, and whether the second attack targets the original vulnerabilities or new unidentified ones. Whereas it is unlikely that a single earthquake will occur around the world (although areas could be affected beyond the immediate earthquake zone), the same cannot be said for a cyberattack.

Cyberattacks and other cyber events are created by humans. Attacks are usually directed at specific targets with a clear outcome in mind (e.g. profiting from the attack, causing damage, responding to political manifestations). Cyberattacks could actually be provoked by the behaviour of targeted companies or governments. In that sense, cyber risk may assume features of endogeneity, thereby losing its idiosyncrasy. Attacks may also have unplanned implications. Cyber risk needs to address both malicious cyberattacks and unintentional events caused by machine or human failure. To date, the majority of cyber events have been aided or abetted by humans intentionally or unintentionally. In comparison, natural disasters are not the direct result of human action. Furthermore, the expected losses from many natural disasters can be better predicted than cyberattacks because conditions and locations exposed to specific types of disasters are well known and constantly monitored.

Historical cyberattack data is limited and not well-structured (with the exception of some limited areas such as breach/confidentiality insurance), while natural disasters are highly scrutinised and catalogued in extensive records. Cyber risks, on the other hand, are relatively new events, and the existing models to assess risk and the information available are still limited.

3.2 Accumulation risk

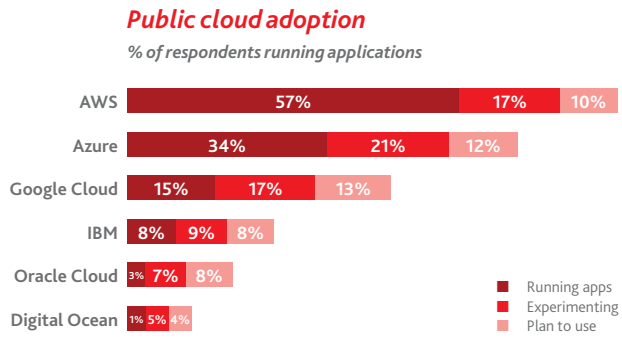
One of the foremost challenges in the cyber security landscape is accumulation risk. There is a great deal of research that addresses this topic. For example, 'Casualty Accumulation Risks'[8] from the CRO Forum and 'Business Blackout'[9] from Lloyd's are two reports that analyse the implications of accumulation risk.

- Accumulation risk is the total exposure affected by incidents (e.g. a cyberattack on a power utility or a cloud service provider) that could cause a significant business disruption or loss across geographies or companies, and affect several insurance policies.

8 http://www.thecroforum.org/casualty-accumulation-risk/
9 http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pd

As more and more companies rely on third-party solutions to operate their businesses (e.g. cloud services from Amazon, Google, IBM or Microsoft; see Figure 1) and interconnectivity increases, accumulation risk is becoming more relevant. The number of companies using common platform software (e.g. SAP) or moving to the cloud increases the potential impact of a large-scale attack. During our interviews, 90 per cent of our respondents mentioned accumulation risk as a critical challenge in the industry, highlighting the importance of assessing and managing this type of risk. From a risk management perspective, if cyber knowledge is inexistent or significantly limited in a company, particularly in SMEs, a better risk mitigation strategy might be to rely on professional vendors, assuming that the necessary controls, roles and responsibilities are put in place. That said, vendor management is also an important means of managing accumulation risk.

Figure 1: Public cloud adoption.



Source: interviews.

Accumulation risk has become a top priority for insurance companies; however, many customers are still not fully aware of its potential impact.

Amazon Web Services (AWS) is one of the largest cloud providers. In the hypothetical case of an attack against AWS, many companies using AWS would be affected. The potential impact could range from business interruption to PP&E damage, casualties, etc. The complexity of accumulation risk means that it is not clear whose insurance would cover what in the case of such an attack. Should AWS's insurance cover all affected customers? Should the insurance of the affected customer be responsible? Should a cyber or PP&E policy cover associated losses?

Accumulation risk is not the only consequence of exposure to the cloud. Companies using the same IT platforms and tools are all exposed to the vulnerabilities of those platforms and tools (e.g. SAP vulnerabilities can affect anyone using SAP). For example, in a recent cyberattack on a post-production sound editing studio, several television shows and movies were stolen.[10] The footage belonged to different studios (ABC, Netflix, Fox), but because all of them were using the same sound editing studio, they were exposed to the same attack. Initially, the hackers demanded a ransom from the audio studio, but the studio refused to pay. Clearly, the implicated parties effectively lost their movies as they were released on the internet, but what is not clear is whose insurance is responsible for covering the incident.

All the above-mentioned issues illustrate the complexity of accumulation risk. Four out of the ten insurers interviewed had decided not to cover risks associated with cloud or software vendors. As for the reasons for not covering accumulation risk, two interviewees cited the difficulty in measuring and predicting its impact. Insurance companies that cover accumulation risk are spending a significant amount of their time educating their customers, focusing on illustrating how the usage of extended IT infrastructure and tools represents a vulnerability for a company and how companies can be better prepared to deal with such exposure. Our interviewees noted that the way underwriters perceive accumulation risk is similar to how they perceive a pandemic scenario. In fact, this analogy was used to educate cyber insurance customers on the relevance of this type of risk.

Insurance companies also mentioned that it is difficult to price accumulation risk. To this day, there has not been a major, systemic cyber incident that has provided sufficient data to be included in insurers' cyber risk models. The lack of data and the many interdependencies between companies make it difficult to assess the ultimate impact of such an event. Nevertheless, some insurers and reinsurers are willing to take on this risk. If insurers want to

10 http://fortune.com/2017/05/01/netflix-orange-new-black-hack/

be able to successfully manage the potential of extreme losses associated with accumulation risk, the industry needs to create better risk models and educate customers to help them understand their accumulation risk exposure.

3.3 Limited data availability and information sharing

Like technology itself, cyber risks evolve.[11] Every week, or even every day, new vulnerabilities and types of attacks are discovered. There are groups who are fully dedicated to finding and exploiting vulnerabilities. Once a vulnerability is detected and made known, it may become obsolete rather quickly, so hackers keep looking for new vulnerabilities. Hackers have substantially advanced a variety of social engineering capabilities, including, for example, sophisticated phishing campaigns that trick even cautious users into clicking on links that provide system access to attackers. Known vulnerabilities and the human factor remain the cause of most attacks.

Sharing incident data and the resulting claims information would help to provide much needed historical data to build or enhance cyber risk models. This would in turn help insurers to improve their pricing methodology and identify gaps in customers' security. A common repository of incident data could also help to raise cyber awareness across customer organisations. As more information about cyber incidents is added to the repository, companies would be better informed about their exposure to cyber risks. Greater awareness could result in greater demand for cyber insurance and lead to improved market efficiency. Finally, cyber insurance companies could alert their customers to potential incidents or even vulnerabilities based on the incident data from similar organisations.

Currently, cyber risk data is limited. There is less historical data available for cyber incidents and claims than for traditional insurance claims. Companies are wary of putting their cyber incident data into a common repository due to multiple factors: (1) even if the data is anonymised, it is frequently distinct enough to be traced back to a specific company; (2) exposing this data may make the company attractive to further attacks or expose it to regulatory fines or legal fees; (3) once placed in a repository, the data may be passed to supervisors or published without the owner's consent. While legal structures that facilitate cyber information sharing—e.g. providing limited liability protection in case of inadvertent disclosure of private information—have improved in the past two years, they are still evolving. This is complicated by different countries and regions enacting their own laws, creating a patchwork of inconsistent rules and regulations. Within Information Sharing and Analysis Centers (ISACs), sharing is restricted to the closed environment and does not include insurance claim data. Finally, there is no single data structure that allows cross-industry sharing, and only limited standards that describe and codify different types of incidents.

Nowadays, cyberattacks are happening more frequently and are having greater impact. While data can be extracted from these incidents, cross-industry sharing of the data and gaining insights from it pose key challenges. Companies are concerned about the negative implications of publicly disclosing their vulnerabilities (e.g. public perception or reputation could be impacted). Sometimes, companies are not allowed, or not willing to take on the risk of disclosing past attacks due to the existence of regulations or contracts. For instance, if the event is under investigation by law enforcement, the company will be banned from releasing details regarding the investigation and will therefore not be able to share any data about the attack. Until there is a framework that allows satisfactory sharing of cyber incident data while limiting the potential liability of involved companies, the current situation will not improve.

Insurers have the option to collaborate and share their data, but in most cases, they simply do not do it. None of the insurers interviewed are currently sharing their incident information, although two out of the ten mentioned that they are actively collaborating on defining mechanisms to share information. Five out of ten believe that sharing information would be beneficial to the industry. However, the insurers who did not support sharing mentioned that their incident data constituted their own competitive advantage, so it would not be beneficial for them to share it.

There are several efforts facilitated by governments and the insurance industry to create a common repository

11 http://web.mit.edu/smadnick/www/wp/2016-10.pdf

and to standardise the classification and reporting of cyber incidents. The ultimate goal is to provide insurance companies and organisations with access to cyber incident information that would help them to better assess their risk and implement appropriate mitigating controls. One of the most important initiatives is CIDAR[12] led by the Department of Homeland Security in the U.S. The CRO Forum[13] is also involved in improving the categorisation and reporting of cyber risk, working closely with different insurance companies.

3.4 Impact of cyber regulation

The main difference between the U.S. and Europe is the role that regulation has played in the development of the cyber risk market. There are two relevant developments. The first, and so far relatively well-advanced development, concerns the treatment of cyber incidents in the corporate sector (including financial services) and the protection of consumers with respect to the protection and integrity of data stored in the cyber space. The second relates to the regulation of insurers as providers of risk solutions to their customers. This regulatory development is still in its infancy.

With regard to the first developments, and according to the participants in our interviews, the U.S. cyber insurance market is a couple of years ahead of the European market. The main reason is that regulation in the U.S. has driven the market to increase its demand for cyber risk coverage: in the U.S. market, companies are required to report cyber incidents (i.e. a data breach) to their customers and to the authorities.

The European regulatory landscape is about to change with the introduction of the General Data Protection Regulation (GDPR) in May 2018.[14] Insurance companies writing cyber policies expect that the new directive will boost the market to levels similar to those of the U.S. market. The new regulation will help to raise cyber awareness on the customer side and increase efforts to protect customer data, raising demand for cyber risk coverage. This imminent change is transforming the market: insurance companies that were not yet in the cyber risk market are developing cyber products, and those already offering cyber products are revisiting and improving them, putting to use their experience and expertise in cyber insurance. We are about to witness an exciting transformation in Europe as the market expands.

With respect to insurance regulation, authorities have recognised that cyber risk has taken on a global dimension and ideally needs to be addressed in a globally coordinated manner. An example is the declaration of EU and U.S. authorities made in early 2017 in which they declared cyber risk as one of the key initiatives in the joint EU-U.S. Insurance Project.[15] However, both the Financial Stability Board (FSB) and the International Association of Insurance Supervisors (IAIS) have so far refrained from developing concrete standards. The FSB has published a stocktake on cybersecurity regulatory and supervisory practices.[16] While FSB member jurisdictions have been active for some time in addressing cybersecurity, nearly three-quarters of members reported plans to issue new regulations, guidance or supervisory practices that address cybersecurity for the financial sector within the next year. The IAIS has released a descriptive analysis with a focus on cyber risks affecting the insurance sector.[17] In this paper, the IAIS indicated that up to eight Insurance Core Principles, which provide a globally accepted framework for the supervision of the insurance sector, will probably need rewording.

That said, a number of national initiatives are more specific. The U.K. Prudential Regulation Authority, for example has issued a consultation paper on 'Cyber risk underwriting risk' that is mainly concerned with issues of accumulation risk and silent risk.[18] It is clear that national authorities will soon issue guidance and regulations on the topic of insurers active in the cyber risk transfer market.

12 CIDAR(Cyber Incident Data and Analysis Repository), https://www.dhs.gov/event/cidar-workshop
13 http://www.thecroforum.org/concept-proposal-categorisation-methodology-for-cyber-risk/
14 http://ec.europa.eu/justice/data-protection/reform/index_en.htm
15 https://eiopa.europa.eu/Publications/Press%20Releases/2017-01-17%20THE%20EU%20–%20U.S.%20INSURANCE%20PROJECT%20ADDRESSES%20CYBER%20RISK.doc.pdf
16 Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices, available at http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/
17 Issues Paper on Cyber Risk to the Insurance Sector, available at https://www.iaisweb.org/page/consultations/closed-consultations/issues-paper-on-cyber-risks-to-the-insurance-sector
18 Cyber insurance underwriting risk, available at http://www.bankofengland.co.uk/pra/Documents/publications/cp/2016/cp3916.pdf

There are also private-public partnerships in the area of standard setting. The Cyber Risk Management project (CyRiM) based in Singapore represents a partnership between the Monetary Authority of Singapore, Nanyang Technology University and major insurers, reinsurers and brokers.[19] It seeks clarity on the definition of cyber risk, creating a common data set, exploring loss scenarios, creating benchmark loss models, and considering methods for non-intrusive risk assessment.

Despite the role they have played so far, insurers and their customers should not wait for regulation to force them to start thinking about cyber risk. The corporate sector, and especially small and medium-sized companies that do not yet have cyber insurance, should explore this possibility.

3.5 Technology and cyber insurance

Technology and cyber risk go hand in hand. As technology improves and transforms our lives, hackers are getting more and more sophisticated, developing attacks that could potentially destroy companies and governments. With the expansion of the Internet, the proliferation of smart connected devices (Internet of Things (IoT) devices) and the rise of autonomous vehicles, there is an increasingly large number of possible attack vectors, and an increased potential for a point of failure that could lead to a disastrous scenario.

Cyber vulnerabilities can affect the success of new technologies

The cyber risk analysis market is evolving as rapidly as the technology market itself. In fact, there are numerous start-ups focused on risk modelling and risk ratings that are helping to improve cyber insurance risk models. Examples include Bitsight, Security Scorecard, and FICO security score. As another example, Swiss Re has recently partnered with Cyence to improve their risk modelling tools.[20]

Cyber insurance should foster and support the advancement of new technologies that safeguard their customers' new products. Insurers active in the cyber market should support the development of tools that can reduce the risk and exposure of their customers. Some companies are already investing in new technologies to monitor their customers' network activity and to predict future attacks with machine learning algorithms. Many cybersecurity companies are also focusing on automating cybersecurity operations to quickly identify and remove vulnerabilities and to measure the quality of security measures they have implemented.

Finally, insurers could assume an important role in the propagation and enforcement of minimal IT security and information security standards. They could do so by varying the terms and conditions of cyber policies, depending on the degree of sophistication of IT protection and IT governance assessed for customers. This would not only benefit corporate customers but also protect society and improve the resilience of an increasingly interconnected world.

19 http://irfrc.ntu.edu.sg/Research/CurrentProjects/Pages/Cyber-Risk-Management-Programme.aspx
20 Swiss Re Sigma no 1/2017 report; https://www.cyence.net/

4. The insurance role in cyber risk transfer

Cyber insurance is an immature, yet quickly evolving market. Insurance companies are still entering and learning the market, while customers are either sceptical or unsure of the potential of the market. Nonetheless, it is now clear that the market will grow in the coming years.

According to the most recent reports, the size of the cyber insurance market is believed to be about USD 3 billion. The attractiveness of the market is clearly shown by the number of insurance companies that are continuously entering the market with new products. In our interviews, several insurers mentioned that they were revisiting and relaunching their cyber insurance products to make them more attractive to their customers, and companies that originally did not want to join the cyber insurance market have already entered it or have plans to enter it.

The main reason for this trend is that the cyber insurance market has become profitable due to the still limited number of claims. Additionally, some customers purchase cyber insurance to satisfy industry-specific regulations or requests from executive boards, never intending to file a claim. Some insurers expect profitability to level off as the balance between policies written and claims incurred will likely change in the near future.

As the market keeps growing, competition will increase. To secure their market share, underwriters must better understand their customers and design policies that match their needs. From our interviews, it is clear that insurers already distinguish between large companies and SMEs, each with different needs and degrees of exposure to cyber risk (see Figure 2).

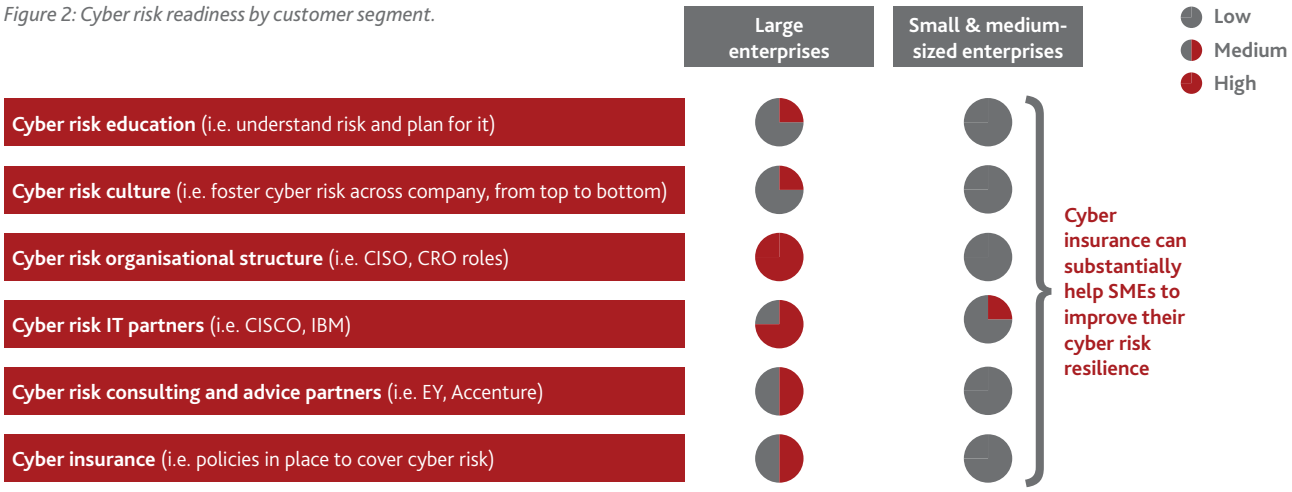
There are two clear customer size segments in the cyber insurance market: large enterprises and small/medium enterprises

On the one hand, there are large enterprises, such as financial institutions (e.g. HSBC, Citibank, State Street), that have large IT departments and dedicated resources to manage risk. These companies usually have in their organisation a Chief Risk Officer and Chief Information Security Officer who are well prepared to deal with cyber risk and have a high degree of understanding of their vulnerabilities and exposures. In addition, large companies usually have cyber insurance policies and work with external cyber risk consultants to reduce exposure.

SMEs are not ready to deal with cyber risk, making selling cyber insurance to them a slow and costly process

On the other hand, SMEs populate a very different landscape. While there are notable exceptions, SMEs as a group lack the expertise and resources to deal with cyber risk effectively. They are usually unaware of vulnerabilities and risk exposures, they do not have dedicated teams to deal with cyber risk, and even when they do, the team

Figure 2: Cyber risk readiness by customer segment.



Source: Interviews.

is neither large nor diverse enough to provide adequate protection. As a result, SMEs outsource much of their IT and cybersecurity functions. While this market has an attractive potential for cyber insurance, underwriters find it difficult to demonstrate the value of insurance to SMEs that are not well versed in cyber risk. The investment of time that would be required for insurers and brokers to sell to SMEs is substantial, and returns can be small. Some interviewees pointed out that the sales process of cyber insurance is slow and costly. It starts with creating cyber awareness and teaching the customer how to assess their exposure.

This begs the question, what can underwriters and brokers do to attract cyber insurance customers? The first trend that we have observed is the need to clearly define which insurance policies address cyber risk. The current practice is to either include cyber risk cover as a part of existing policies or as stand-alone insurance products. We have heard in our interviews that it is difficult to understand which policies cover which events, and that better clarity is needed to increase customer awareness and understanding of cyber insurance options. The second trend concerns the standardisation and simplification of cyber insurance language. Customers who are not well versed in cyber insurance find it difficult to understand policies and premiums. The provision of education by underwriters and brokers is important for this process. Third, insurance companies are already working to demonstrate how cyber insurance can add value to organisations beyond just providing coverage.

4.1 The expanding role along the value chain

Cyber insurance companies are experiencing a **symbiotic transformation of their business model, including more services along the value chain.** Insurers are moving from providing simple risk transfer options to offering risk consultation and prevention and breach resolution services (see Figure 5). Underwriters are transforming their role, shifting their value proposition so that they are present along the entire value chain of their customers:

- **Pre-breach:** Insurers are working to design appropriate cyber insurance policies for their future clients. They are working with customers to better understand risks and to prevent breaches based on appropriate risk management frameworks. Insurers are also offering consulting services to train and assist organisations in best practices for reacting to and limiting the damage from a cyberattack or incident.

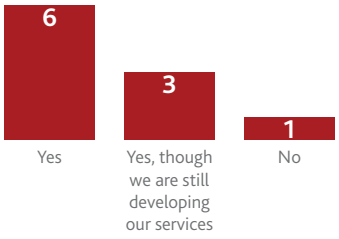
- **Post-breach:** Insurers are providing services that evaluate the impact of an attack, help implement response and recovery plans, provide public relations and communications support, and identify appropriate mitigating actions.

In the past, insurers were present only after a breach. Underwriters helped with claims and coverage, but did not actively engage or collaborate with their customers on how to improve their cyber risk practices. Enterprises have traditionally hired IT vendors, consulting firms and specialised cybersecurity firms to address their cyber risk management needs. Today, the insurance industry is experiencing a transformation to a situation where insurers and customers become partners in reducing cyber risk exposure and the potential losses associated with it.

Insurance companies are building cyber risk expertise to better serve their customers. The additional services offered by insurance companies range from cybersecurity training to incident resolution advice and forensics after a cyber event.

Figure 3: Companies interviewed that provide value-added services with their cyber insurance.

Is your company providing value-added services with your cyber insurance offer?
# of respondents (10 responses in total)



Source: Interviews

Figure 4: Companies interviewed that provide value-added services with their cyber insurance.

Reasons to provide value-added services
# of respondents (10 respondents, multiple answers)

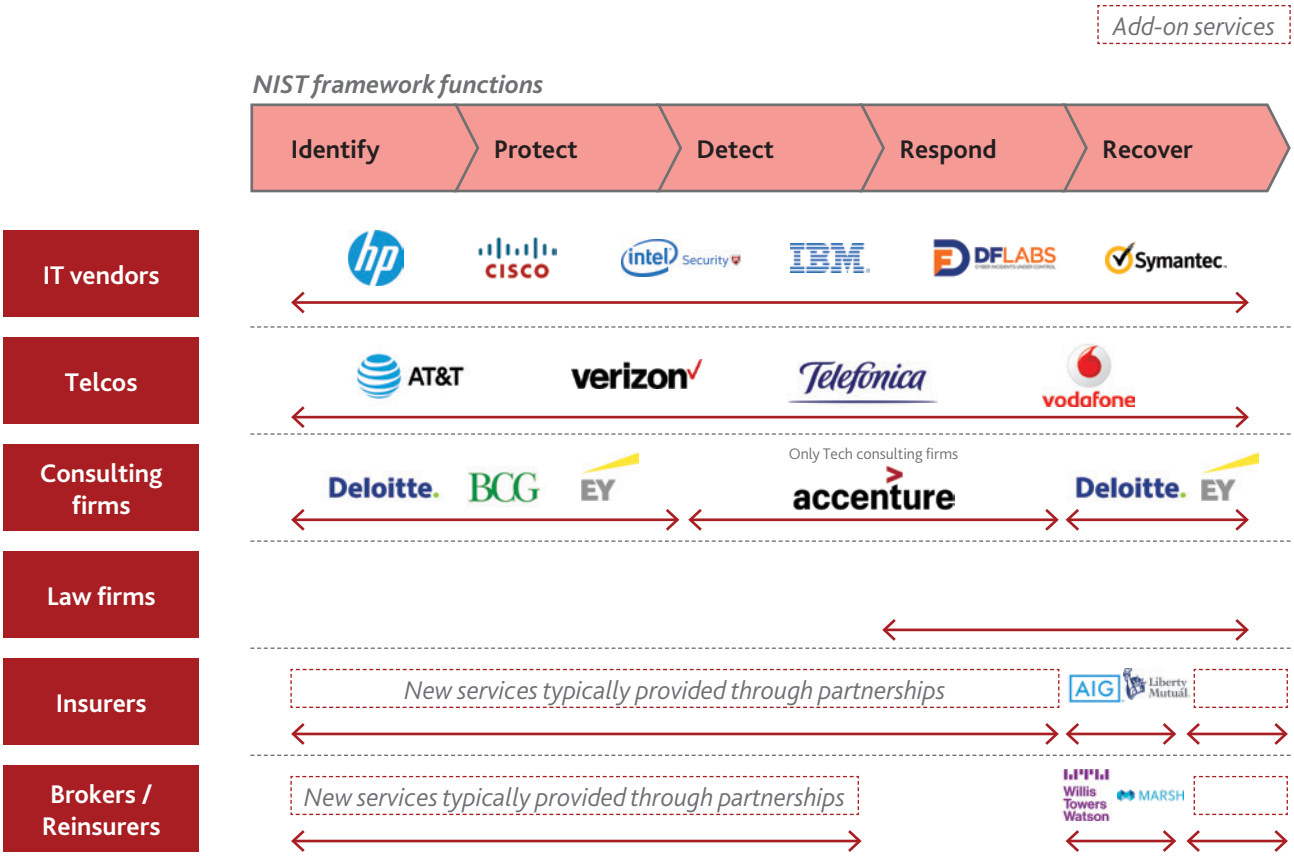
Source: Interviews

According to our interviews, **customers are aware of these new additional services and some customers want greater involvement from their cyber insurer.** Half of the customers we interviewed mentioned the use of cyber insurers' services, and one of them indicated that the company would love to have even a higher involvement with their cyber insurance provider. As we mentioned earlier in this report, large enterprises already have tools, mechanisms and partnerships with cyber security experts. They are well informed and they know how to assess and prevent risk. SMEs lack the resources and capabilities required to successfully reduce their cyber risk exposure. Cyber insurance can add more value, connecting SMEs with the right partners, providing useful advice and helping them manage and reduce their cyber risk. As one reinsurer mentioned *"small and medium companies are overwhelmed by cyber risk. After an attack they don't even know how to submit a claim. They need our help"*.

Cyber insurance provides the tools and knowledge to manage cyber risk

The new role of cyber insurance is driven by three market needs: (1) increasing attractiveness of cyber insurance for customers; (2) improving profitability through loss reduction/prevention and customer retention; and (3) gaining cyber risk knowledge (see Figure 4).

Figure 5: Cyber risk value chain (non-exhaustive).



Source: BCG Platinion

The addition of new services along the cyber risk value chain increases the attractiveness of cyber insurance for customers and potentially improves the profitability of insurers

The additional services along the value chain generate fee income and help reduce the probability and size of losses, making it in the interest of the insurers and brokers to prepare and help their customers to manage risk. This point was highlighted by all interviewees who were offering these additional services at the time. Customers who have a risk management plan, risk prevention and resolution tools, as well as dedicated teams in their organisations are better prepared to deal with cyber risk. Offering additional services also increases customer retention. The long sales process and the required upfront investment in a customer incentivises insurers to cultivate a long-lasting relationship with the companies they cover.

Establishing a presence in all phases of the cyber risk value chain enables insurers to capture more insights and knowledge from the market. Insurers with an understanding of the market, its customers and cyber risk are better prepared to design risk models and pricing frameworks. Ultimately, engagement in the entire value chain is a competitive advantage for insurers. As mentioned in Section 3.3: *Limited data availability and information sharing*, information about cyber risk incidents is limited, and no common repository exists yet, although efforts to create one are ongoing. Having control of information along the entire value chain will help insurers to better diagnose the causes of an attack, analyse

resolution scenarios, and, ultimately, will help their customers to successfully manage cyber risk.

Cyber risk services offered by insurers are usually provided through third parties

The great range of new services offered through the cyber insurance value chain is usually set up through partnerships with third-party providers (e.g. IBM, FireEye). All interviewees implementing value-added services indicated that they offer them through third parties, with only three out of ten interviewees stating that they are developing in-house capabilities. In most post-breach cases, insurers refer customers to partners who deliver the services. Pre-breach services, such as cybersecurity training, may be provided as a part of the overall cyber insurance policy. Insurers and brokers are hiring cyber experts, and even funding or acquiring cyber risk companies to better advise their customers. The acquisition of a leading cybersecurity firm, Stroz Friedberg Inc., by AON in 2016, is an example of this trend.[21]

Insurers are developing competitive advantages by providing access to innovative services and technologies in addition to traditional insurance. An example from our interviews was installing network sensors on a customer's premises to detect network vulnerabilities using machine learning algorithms.

4.2 Coordinating the cyber insurance ecosystem

These new services along the value chain are not without risks and challenges for the insurance companies themselves:

1. Insurance companies need to ensure that the third-party companies with which they partner actually deliver. Any discontent with third-party providers will impact the insurance company; for example, if a third-party service is not able to provide appropriate forensics or post-breach communication support to a customer, the customer may hold the cyber insurance provider accountable.
2. A closer relationship with customers means knowing more about them, but insurers risk being perceived as too controlling or meddlesome. Cyber insurance customers are already wary of sharing more than is required, so cyber insurance companies need to communicate to their customers that sharing information is for their own benefit, and highlight the advantages of good relationships.
3. Attracting SMEs with a combination of services will require a new sales process. SMEs are more inclined to allow insurers/brokers access to their network and will accept more services from them because SMEs are lacking in their own cybersecurity efforts, as discussed earlier in this paper.

4.3 Improving customers' cybersecurity

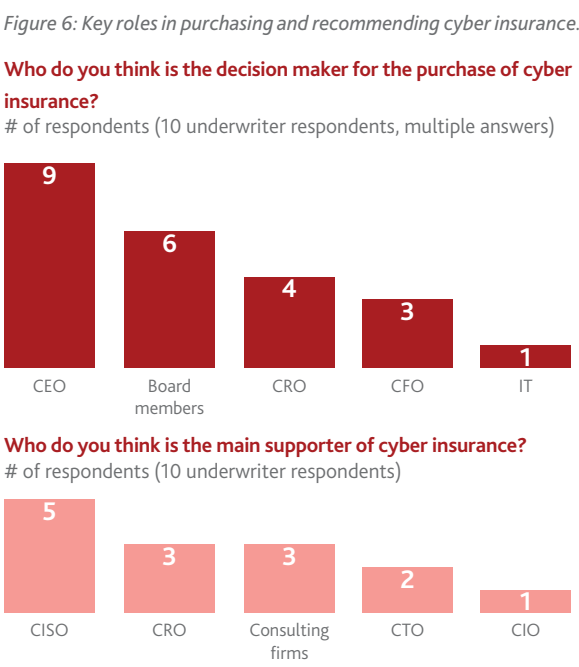
Insurance companies active in the cyber market have an opportunity to help their customers better manage cybersecurity risk by enhancing cyber risk communications in customers' enterprises.

Executive management and board members are the key decision makers in purchasing cyber insurance

The order to take out a cyber insurance policy frequently comes from managers at the highest levels of a company (e.g. CEO, CFO) or from the Board of Directors (see Figure 6).

21 https://www.wsj.com/articles/insurance-broker-aon-acquires-cyber-risk-specialist-stroz-friedberg-1476178202

Figure 6: Key roles in purchasing and recommending cyber insurance.



Source: Interviews

The role of the CISO or Head of Security varies from company to company.[22] The objectives of the CISO are to effectively and efficiently protect critical enterprise information and improve cybersecurity practices. While CISOs are generally aware of cyber insurance as a valid risk transfer option, it remains outside the mainstream. Today, CISOs prefer to manage cybersecurity risks by implementing robust processes, hiring qualified employees, and purchasing appropriate technologies to protect the enterprise. Because CISOs are the target of the expanded service suite that insurers are beginning to offer, insurers need to figure out how to gain CISOs' trust and support. Some of our respondents stated that *"the CISO does not want to hear that he is doing a poor job, so insurers need to work with him and go beyond just mentioning their gaps."*

The role of the CRO or risk manager is different from that of the CISO. While the CISO focuses on creating a strategy for planning and executing security measures to reduce cyber risk, CROs (or risk managers) focus on establishing overall risk strategies and practices that will minimise the exposure of the company to all risk. The incentives of the risk managers are usually linked with the long-term performance of the company. CROs and risk managers are typically the buyers of insurance in their organisations, making the CRO a natural marketing target for insurers.

Our data indicates that the CISO and the CRO frequently work in different parts of an organisation, sometimes do not know each other and may even use different definitions of risk. This gap represents a challenge for insurers because they sell their product to the CRO, even though the product is likely to be used by the CISO. According to our interviews, half of the insurers believe that there is a lack of communication between CISOs and CROs. This represents a unique opportunity for insurers who could help to bridge that gap, and by doing so, increase demand for cyber insurance and the value-added services that insurers now provide. Cyber risk insurers can help the CRO and the CISO break company silos and collaborate on cyber insurance.

Getting to the CISO or the CRO is just the first step for insurers. Underwriters and brokers need to demonstrate to the CISO and CRO the value that cyber insurance can bring to the company before these managers in turn can support it in front of the CEO. To do so, insurers should use their qualification processes to provide meaningful insights into the customer's cybersecurity. Insurers can also host workshops for both CISOs and CROs to create a common understanding and lexicon among those two groups of leaders, connect potential customers with existing ones, and educate them about cybersecurity and the benefits of cyber insurance.

Insurers need to demonstrate the value of cyber insurance to CISOs to increase the use of cyber insurance.

The purchase of cyber insurance is just one of the steps in reducing cyber risk.

Insurers need to continuously train and educate their customers in cyber risk. Insurers do not need to be the provider of the training content or products, but they can direct their customers to sources that provide the right education and services to help improve cyber risk knowledge and practices.

22 https://blogs.wsj.com/cio/2017/05/05/thomson-reuters-ciso-cybersecurity-leadership-brings-personal-professional-challenges/

Cyber security needs to be championed from the top, down (i.e. starting at the CEO level and extending to all employees). There are a lot of discussions about where risk and security managers should be positioned in the organisational structure. In our interviews, one underwriter expressed his concerns that CISOs and CROs were not operating at senior enough levels to make a difference: "in the past years, CISOs and CROs have been downgraded and their access to the top level is becoming more limited". Some reports that we have reviewed stated that the CISO should report to the CRO instead of reporting to the CIO. This recommendation is based on the fact that they share many goals when it comes to managing risks the company faces.

In our view, regardless of how the relationship between CISO and CRO is structured, **insurers should foster the inclusion of both CISO and CRO in the executive committee or at the senior management level.** We believe that this new structure will send a clear signal throughout the organisation and to the market that cyber security is a top priority. Risk and security managers already understand cyber risk, and giving them the opportunity to share their knowledge and expertise with top managers will help foster a cyber security culture within a company. Numerous reports, industry documents, standards and guidelines, and our own interviews make it clear that top management needs to lead the transformation and set an example for the company to follow. Once the top management is aware of cyber risk, the message needs to be carried forward to the rest of the company by multiple means, including through role modelling by top managers. Cyber insurance can help make this happen by defining the optimal mechanisms and strategies to spread cyber awareness.

Underwriters should constantly test and assess their customer risk capabilities. Training is essential, but without practice, lessons will not be learned.

Insurers need to advise their customers that employees are accountable for cyber risk. Employees need to understand that cyber security is a part of business, and that they must be committed to following appropriate cybersecurity practices. This is a critical part of a successful cybersecurity culture (in which the companies need to be involved as the main promoters).

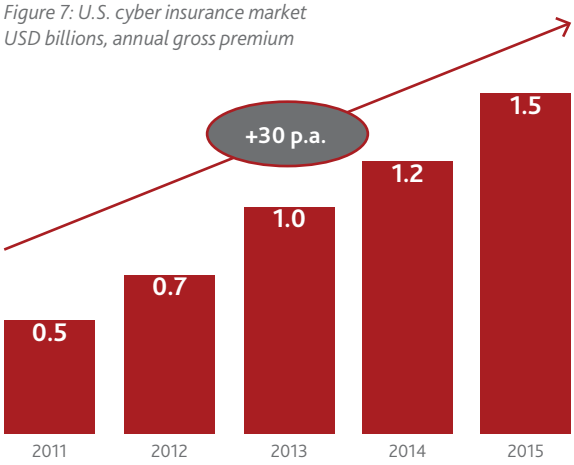
Lastly, insurers should provide help and guidance through their additional services (see Section 4.1: *The expanding role along the value chain*). Before, during, and after a cyberattack, insurers need to provide the right tools to help to manage cyber risk. For example, insurers can inform customers of recently discovered vulnerabilities that are applicable to the customers' environments, suggest implementation of general best practices, and inform customers of new security solutions that can reduce cyber risk.

Cyber insurance companies are expanding their services to include options along the entire cyber risk value chain. Insurers are offering new services, from prevention to mitigation and resolution through third-party partnerships, and are cultivating deeper relationships with their customers to better prevent cyber risks. Cyber insurance companies need to continue to follow this trajectory to maximise market growth opportunities through increased customer value.

5. The growing cyber insurance market

Most of the cyber insurance market is in the U.S., where, according to various estimates, premiums range from USD 1.5 billion to USD 2 billion annually (see Figure 7). Roughly half of this premium volume is written as stand-alone cyber security insurance products, while the other half is part of a more general property and casualty package policy.[23] The U.S. market is dominated by three main carriers that control almost half of the market (see Section 5.1. *Differences in regional markets*); however, the market is constantly expanding, with an annual growth of more than 25 per cent according to some interviewees.

Figure 7: U.S. cyber insurance market
USD billions, annual gross premium



Sources: SCOR, AON, McAfee

There are several signs of the cyber insurance market's relative immaturity. First, there is a lack of standardisation of insurance offerings. Some insurers offer stand-alone policies, creating a clear separation between their traditional policies and cyber insurance policies. Other insurers have decided to embed cyber in their existing coverage (e.g. including cyber clauses in PP&E coverage); this represents a different philosophy, driven by the argument that this option is easier to sell to customers than a whole new type of insurance. However, embedding cyber insurance in other coverage may lead to a lack of clarity about what is and is not covered. In addition, the rapidly evolving nature of cyber risk makes it difficult even for insurers themselves to define what is and is not covered.

Second, insurers active in the cyber market for the first time tend to focus only on common cyber risk events (e.g. notification costs) because they have neither sufficient data nor experience to price and model more complex cyber risks. By offering these limited policies, insurers can further develop their cyber risk expertise to later expand their services.

Third, the services provided by new entrants to the cyber insurance market may not be sufficiently robust and may not be able to provide adequate support when a cyber incident occurs, compared to the services of insurers that entered the market early, have had time to develop sophisticated pricing models, and already possess advanced risk modelling tools to calculate premiums. Established insurers understand their customers' risks and are careful when assessing them. Customers may have to go through detailed assessments, including responding to NIST Cybersecurity Framework-like questionnaires and producing or allowing automated scores to be used. However, new insurers who enter the cyber insurance market with less robust knowledge of the topic usually use shorter questionnaires to assess customers.

5.1 Differences in regional markets

Our sources cited that the existence of strong cybersecurity and data breach reporting regulations, the presence of high-impact cyber incidents, and the growth in cyber-related litigation have accelerated growth of the U.S. cyber insurance market. Another important factor in this trend is how many of the world's largest enterprises operate in the U.S. market. These large companies have dedicated cyber security teams and sophisticated cybersecurity leaders who understand cyber risk and want to transfer part of that risk by using insurance. That said, there is still a lot of room for growth.

The U.S. is the biggest cyber insurance market, but Europe and Asia are catching up due to new regulations and recent attacks

Meanwhile, in Europe, insurers are still developing their cyber offerings. Traditionally, global insurers have been repackaging their U.S. cyber offerings for Europe, but as many of our interviewees mentioned, this approach

23 See NAIC at http://www.naic.org/cipr_topics/topic_cyber_risk.htm

has had only a limited effect in satisfying the needs of European customers. Insurers are now focusing on developing cyber insurance offerings that target European priorities, regulations and cultural norms. Moreover, the 2018 European data protection regulation (GDPR) is expected to stimulate the European cyber landscape.[24] Almost half of the surveyed insurers stated that GDPR will act as a trigger for the European cyber insurance market. The regulation requires that companies report to their customers within 72 hours any data breach that "results in a risk for the rights and freedoms of individuals." The failure to comply with GDPR can result in high penalties of up to 4 per cent of annual global turnover or EUR 20 million (whichever is greater). These rules apply to companies controlling and using customer data as well as the enterprises in charge of transferring data (cloud services or network providers).

The Asian market is still in its early phases; Asian companies are aware of cyber risk but are not ready to take full advantage of cyber insurance. In our conversations with insurance companies present in Asia, they highlighted that customers are demanding policies that help them to deal with data breach notification costs.

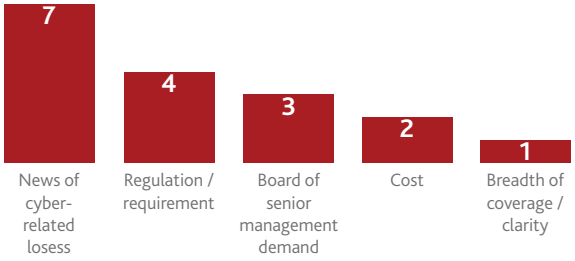
5.2 Understanding the future of the market

According to a recent report from PartnerRe, the main drivers of the cyber insurance market are news about cyber incidents, and external requirements such as those from regulators or customers (see Figure 8)[25].

Interviewees said that awareness of attacks is a strong market driver, citing the Target and Sony attacks that led to the adoption of new policies. As we discussed in the previous chapter, regulation is considered to be another key market driver.

Figure 8: Drivers of the cyber insurance market

What do you see as the top driver of cyber insurance sales?
% (interviews with 15 underwriters and customers)



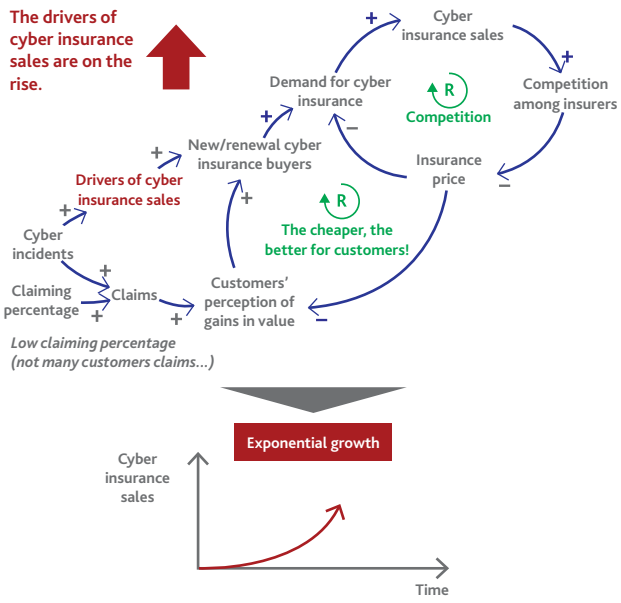
Source: PartnerRe 2016 survey report

Cyber incidents and third-party requirements are the main drivers of cyber insurance sales

With the help of an MIT expert in system dynamics, we have developed a preliminary model of the behaviour of the cyber insurance market (see Figure 9). We created a simple representation of the market where the above-mentioned drivers and the low percentage of claims are increasing the demand for cyber insurance. As demand increases, over time new insurers will enter the cyber market, eventually lowering prices due to competition. This situation will have a positive impact on the way customers perceive value, which in turn will be translated into more demand for cyber insurance. This positive loop and the increase in cyber insurance drivers will lead to a growing market (if nothing else is considered).

24 http://ec.europa.eu/justice/data-protection/reform/index_en.htm; http://www.eugdpr.org/the-regulation.html
25 http://www.partnerre.com/assets/uploads/docs/PartnerRe_Cyber_Liability_Trends_Survey_2016.pdf

Figure 9: A simple representation of the cyber insurance market

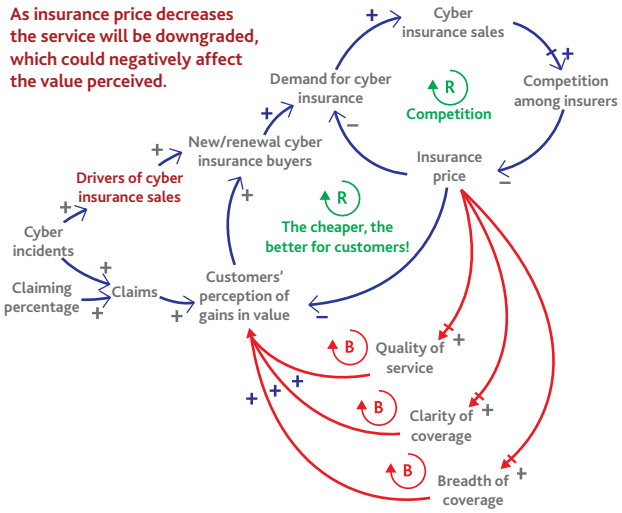


Source: MIT-(IC)[3]

The reality is more complex, however. There are many balancing forces in the market that will counter this positive trend (see Figure 10). For example, as the price of insurance drops, there is a risk of (1) lowering the quality of the service offered and (2) reducing the breadth of coverage of current policies. If the cyber insurance offer is downgraded, the perceived value of the product will decrease, and demand for cyber insurance will be reduced.

The consequences of the balancing forces in the market are that the evolution of the market in the coming years will depend on how underwriters assess the trade-off between coverage and price. Difficulties in the market can occur if insurers and other market stakeholders do not design and implement effective long-term strategies that incorporate the reinforcing and balancing forces (see Figure 10).

Figure 10: Cyber insurance market model including balancing forces



Source: MIT-(IC)[3]

Further research is needed in this area to better understand the dynamics of the insurance market and define strategies to help the market achieve its full potential.

6. Final words

Cyber insurance is the fastest growing line of business in the insurance industry. There is a major opportunity for the industry to provide cyber risk transfer in the form of cyber insurance policies and to mitigate the impact of a cyberattack through prevention, detection and response services. These areas are not new to insurers or the organisations working with insurers. What is new, however, is the risk associated with the revolutionary digitisation of business activities.

The cyber insurance market is influenced by a series of issues: (1) the unique nature of cyber risk; (2) the difficulty in measuring and understanding accumulation risk; (3) the limited availability and sharing of cyber incidents and claims data; (4) the impact of regulation; and (5) the effect of new technologies on cyber security. Although risk transfer is well understood in the insurance market in general, these specific issues are currently posing new challenges.

The short history of cyber insurance, the incomplete and untested risk models and the possibility of system-wide attacks are hindering the development of the market. The research presented in this paper provides insights into the questions concerning (1) the symbiotic transformation of insurers expanding their services along the value chain; (2) the ability of insurers to improve cyber awareness and remove customers' protection gaps; and (3) an understanding of the dynamics of the cyber insurance market. It also suggests important areas for future research, including:

- **Identifying solutions to the greatest challenges**—Insurability, accumulation risk, capacity constraints, other related unknowns, including modelling capabilities, are some of the greatest challenges.

- **Understanding market dynamics**—Better tracking and prediction of cyber insurance market movement, entry and exit of players, market pricing, cyber risk metrics, and the impact of cyber events.

- **Understanding cyber in terms of other insurance**—What can we gain by looking at other insurance markets and products (e.g. extreme natural catastrophe risks, terrorism and war)?

- **Creating an effective value chain**—Finding the right mix of services, in-house vs partnerships, charging for services, requirement vs voluntary, are just a few of the issues in building the cyber risk service value chain.

- **Understanding the political, micro- and macroeconomic impacts of cyber risk**—Many of the aspects of cyber risk are being played out in the international community in terms of policies, politics, regulations and trade policies. How these will impact insurers today and in the future is a very important aspect of the insurance marketplace.

Insurers are in a unique position to help their customers improve cyber awareness and better understand and deal with cyber risks. In addition to the growth of policies for cyber risk transfer, the cyber risk insurance value chain provides a range of cybersecurity services. This offering serves not only to generate an additional revenue stream and provide greater protection to customers but also allows for the collection of valuable data by insurers regarding cyber risks, cyberattacks, successful mitigation strategies, and the financial impact of attacks.

While risks and opportunities of the nascent cyber market have been identified, the policies developed so far by global standard setters such as the FSB and the IAIS have not kept pace with recent market dynamics. There is more work to be done. The industry should see this as an opportunity to reach out in a cooperative spirit, helping policymakers design regulation that effectively supports the evolution towards a mature cyber insurance market.

References

#	Title	Publisher/ Author	Date	Topic	Source
Industry and institutional reports					
1	2016 Cyber Claims Study	NetDiligence	2016	Cyber insurance report from industry surveys	https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf
2	Ten Key Questions on Cyber Risk and Cyber Risk Insurance	The Geneva Association	November 2016	Report on key open challenges for cyber insurance	https://www.genevaassociation.
3	Cyber resilience: The cyber risk challenge and the role of insurance	CRO Forum	December 2014	Analysis of the CRO role to prevent cyber risk and how cyber insurance can remove the protection gap	http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/
4	Social Engineering Fraud	Advisor	April 2016	Cyber insurance response to social engineering fraud	https://www.ajg.com/media/1698650/2016-advisor-social-engineering-fraud.pdf
5	Terrorism risk insurance	United States Government Accountability Office (GAO)	April 2016	Comparison of selected programmes in the United States and foreign countries	https://www.gao.gov/products/GAO-17-62
6	Cyber/privacy insurance market survey	The Betterley report	August 2016	Report with focus on social engineering fraud coverage, and market analysis via industry interviews	http://betterley.com/
7	The SAFETY Act: Providing Critical Liability Protections for Cyber and Physical Security Efforts	VENABLE LLP	April 2014	Law perspective of the SAFETY act	https://www.venable.com/files/Publication/6c0b031e-c2c5-4029-9ac7-13cb1d8c0d07/Presentation/PublicationAttachment/e81d24a3-fc57-4ece-8e1f-179418baf994/The_SAFETY_Act_Providing_Critical_Liability_Protections_for_Cyber_and_Physical_Securi.pdf
8	Bridging the Insurance/ InfoSec Gap: The SANS 2016 Cyber Insurance Survey	SANS Institute	June 2016	Survey report analysing industry challenges of terminology, assessment/ framework, communications, and investment	https://www.sans.org/reading-room/whitepapers/analyst/bridging-insurance-infosec-gap-2016-cyber-insurance-survey-37062
9	2016 survey of cyber insurance market trends	Advisen; PartnerRE	October 2016	Market trends	http://www.partnerre.com/assets/uploads/docs/PartnerRe_Cyber_Liability_Trends_Survey_2016.pdf
10	Information security and cyber risk management	Advisen; Zurich	October 2016	The sixth annual survey on the current state of and trends in information security and cyber risk management	http://www.advisenltd.com/2016/10/26/2016-information-security-cyber-risk-management-survey/

#	Title	Publisher/ Author	Date	Topic	Source
11	P&C: North American Insight - Digital Disruption in Small Business Insurance	Morgan Stanley	July 2016	Takeaway messages from cyber insurance panel at financial conference: (1) cyber insurance is a growing market, (2) modelling presents underwriting challenges, (3) technology and regulations help to shape the industry	http://media-publications.bcg.com/InsurTech-Disruption-in-Small-Business-Insurance-Final.pdf
12	Cyber Insurance Buying Guide	American Banker Association	2016	Cyber insurance buying guide	http://www.aba.com/Tools/Function/Documents/2016Cyber-Insurance-Buying-Guide_FINAL.pdf
13	Casualty Accumulation Risk	CRO Forum	October 2015	Paper about accumulation risk	http://www.thecroforum.org/casualty-accumulation-risk/
14	How to prepare for the cyberattack that is coming to your company	World Economic Forum; Michael Coden, Stuart Madnick, Sandy Pentland, Shoaib Yousuf	November 2016	Sustainably addressing cyber risk requires an organisation-wide and cross-functional approach, and the integration of cybersecurity and business strategy. Boards and senior management play a pivotal role in creating the organisational and cultural environment for such a joint approach	https://www.weforum.org/agenda/2016/11/how-to-prepare-for-the-cyberattack-that-is-coming-to-your-company/
15	Our critical infrastructure is more vulnerable than ever. It doesn't have to be that way	Nadya Bartol and Michael Coden, BCG Platinion	February 2017	Analysis of vulnerabilities and risks of old technologies present in the power grid and legacy infrastructure	https://www.weforum.org/agenda/2017/02/our-critical-infrastructure-is-more-vulnerable-than-ever-it-doesn-t-have-to-be-that-way/
16	Report to the Presidential Commission on Enhancing National Cybersecurity	Michael Coden and Nadya Bartol, BCG Platinion	Sept. 2016	Importance of cyber-safety culture to improve cyber resilience	https://www.nist.gov/sites/default/files/documents/2016/09/15/bcg_rfi_response.pdf
Insurers, brokers and reinsurer papers					
17	Cyber—the fast moving target	AON	2016	Benchmarking views and attitudes by industry; survey report	www.aon.com/russia/files/Final_2016_Cyber_Captive_Survey.pdf
18	AON Cyber Risk Solutions	AON	2016	Detail of AON cyber insurance offer	http://www.aon.com/risk-services/cyber.jsp
19	2017 Global Cyber Risk Transfer	AIG	2017	AIG US product portfolio brochure, for their advanced coverage	http://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-plus-070616-final-digital.pdf
20	Comparison Report	AON	April 2017	Industry report based on the response of organisations to AON cyber security survey	http://www.aon.com/forms/2017/2017-global-cyber-risk-transfer-comparison-report.jsp
21	2017 Global Cyber Risk Transfer	Marsh	September 2016	Market report from Marsh	https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/MMC-Cyber-Handbook_2016-web-final.pdf
22	Comparison Report	AON; Ponemon Institute	April 2017	Comparison of cyber risk transfer and PP&E insurance	http://www.aon.com/attachments/risk-services/cyber/2017-Global-Cyber-Risk-Transfer-Report-Final.pdf

#	Title	Publisher/ Author	Date	Topic	Source
23	CyberEdge® Risk Consulting Services	AIG	2017	End-to-end cyber risk management solutions	http://www.aig.com/business/insurance/cyber-insurance
24	MMC CYBER HANDBOOK 2016 Increasing resilience in the digital economy	Marsh	September 2016	Market report from Marsh	https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/MMC-Cyber-Handbook_2016-web-final.pdf
25	Marsh cyber echo	Marsh	March 2016	Marsh product portfolio brochure	https://www.marsh.com/pr/en/services/cyber-risk/marsh-cyber-echo.html
26	Managing cyber risk	Marsh	March 2016	Marsh product portfolio brochure	https://www.marsh.com/pr/en/services/cyber-risk/managing-cyber-risk-solution.html
27	Benchmarking Trends: Operational Risks Drive Cyber Insurance Purchases	Marsh	March 2016	Benchmarking trends: operational risks drive cyber insurance purchases	https://www.marsh.com/us/insights/research/cyber-benchmarking-trends-2016.html
28	Facing the cyber risk challenge	Lloyd's of London	September 2016	Cyber risk market report, based on surveys. Focus on data breach	https://www.lloyds.com/~/media/files/lloyds/about-lloyds/cob/cyber/report/lloyds_cyber_surveyreport_v2_190916.pdf
29	Business Blackout	Lloyd's of London	July 2015	The insurance implications of a cyber attack on the U.S. power grid	http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf
30	Lloyd's Cyber-Attack Strategy	Lloyd's of London		Lloyd's cyber risk product brochure	https://www.lloyds.com/~/media/files/the%20market/operating%20at%20lloyds/lloyds%20cyber%20attack.pdf
31	CHUBB Cyber Security brochure	CHUBB	2016	CHUBB product brochure	https://www2.chubb.com/us-en/business-insurance/privacy-network-security.aspx
32	Cyber: getting to grips with a complex risk	Swiss Re institute/ IBM	February 2017	Cyber report on industry challenges (quantification) and trends in cyber risk management	http://media.swissre.com/documents/SRI_sigma1_2017_infographic.pdf
33	Mitigating cyber risk could make a difference of USD 120 trillion to global economy by 2030	Zurich	September 2015	New Atlantic Council / Zurich Insurance Group report uses economic modelling tools to examine how cyber risk costs and benefits affect national GDP under an array of complex scenarios. Building resilience remains a key factor	https://www.zurich.com/en/media/news-releases/2015/2015-0910-01
34	Allianz Cyber ProtectTM	Allianz	2016	Allianz cyber risk product brochure	http://www.agcs.allianz.com/services/financial-lines/cyber-insurance/
35	Allianz Cyber Premium ProtectTM	Allianz	2016	Allianz cyber risk premium product brochure	http://www.agcs.allianz.com/services/financial-lines/cyber-insurance/

#	Title	Publisher/ Author	Date	Topic	Source
36	A Guide to Cyber Risk	Allianz	2016	This report examines cyber risk trends and emerging perils around the globe. It also identifies future mitigation strategies, including the role of insurance	http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf
37	Cyber Liability Insurance	Willis Towers Watson	2016	Willis product brochure	https://www.willistowerswatson.com/en/campaigns/cyber/overview
38	Can Cyber-Insurance Coverage Keep Apace With Cyber-Exposure?	Willis Towers Watson	September 2015	Analysis of readiness to tackle cyber terrorism	https://www.towerswatson.com/en/Insights/Newsletters/Global/emphasis/2015/emphasis-2015-3-can-cyber-insurance-coverage-keep-apace-with-cyber-exposure
39	Cyber Risk for insurers	Willis Towers Watson	August 2016	Companies need to recognise that cyber risk defence requires an enterprise-wide response; it is not just an IT issue	http://blog.willis.com/2016/08/cyber-risk-for-insurers/
40	Cyber risk on the rise: From intangible threat to tangible (re) insurance solutions	SCOR	April 2017	Overview of the market from reinsurance. Extracts from workshops and company leaders	https://www.scor.com/en/file/19208/download?token=lXBp2e_R
Government					
41	Insurance for Cyber-Related Critical Infrastructure Loss: Key issues	Department of Homeland Security	September 2016	Synthesis of key challenges in the cyber security sector from a round-table discussion with customers and insurers	https://www.dhs.gov/event/cidar-workshop
42	Enhanced Cyber Risk Management Standards	Department of the Treasury, Federal Reserve System and the Federal Deposit Insurance Corp	October 2016	Review and proposal of cyber risk management standards	https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf
43	Report on Cyber Security in the Insurance Sector	New York State Department of Financial Services	February 2015	Synthesis of the cyber security survey launched in the financial sector	http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf
44	Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches	European Union Agency for Network and Information sharing	December 2015	Overview of the European cyber insurance market on the challenge of data sharing	https://www.enisa.europa.eu/publications/cybersecurity-information-sharing
45	Enhancing resilience through cyber incident data sharing and analysis	Department of Homeland Security	September 2015	This document enumerates and evaluates consensus data categories that enterprise risk owners and insurers could use to assess risks, identify effective controls, and improve cybersecurity culture and practice	https://www.dhs.gov/sites/default/files/publications/Data%20Categories%20White%20Paper%20-%20508%20compliant.pdf

#	Title	Publisher/ Author	Date	Topic	Source
News and magazines					
46	Best's review on cyber risk regulation	Best's review	March 2017	Several articles and opinions on the cyber security market (trends and challenges)	http://www.ambest.com/review/default.aspx
47	How CIO's prepare for tomorrow's healthcare data breaches	Peter B. Nichol	January 2017	Big challenge in healthcare is dealing with patient data. CIO's are preparing their companies through cyber insurance	http://www.cio.com/article/3152861/security/how-cios-prepare-for-tomorrows-healthcare-data-breaches.html
48	Why the largest insurance companies are pouring into Silicon Valley	Ali Safavi	January 2017	Cyber insurance companies are moving where the new tech companies are located: Silicon Valley	https://techcrunch.com/2017/01/01/why-the-largest-insurance-companies-are-pouring-into-silicon-valley/
49	5 data breach predictions for 2017	Thor Olavsrud	January 2017	Data breach predictions for 2017	http://www.cio.com/article/3155724/security/5-data-breach-predictions-for-2017.html
50	Cybercrime by wired fraud—What's covered?	Stacy Collet	September 2015	Limited coverage of wired fraud under cyber insurance policies	http://www.csoonline.com/article/2978935/cyber-attacks-espionage/cybercrime-by-wire-fraud-what-s-covered.html
51	Time to Team Up	Best's Review Magazine, Lucy Pilko, Michael Coden and Michael Schachtner	July 2017	Insurers see strong growth in writing cybersecurity coverage for businesses, but the real prize will go to those insurers that successfully join forces with IT security firms or otherwise provide services to create more value for their corporate clients.	http://www.propertycasualty360.com/2014/12/18/sony-pictures-holds-60-million-cyber-policy-with-m?slreturn=1491085049
Academic papers					
52	The Security Expertise Assessment Measure	Ms. Smith	September 2015	Case analysis	http://www.networkworld.com/article/2984989/security/cyber-insurance-rejects-claim-after-bitpay-lost-1-8-million-in-phishing-attack.html
53	Modeling Cyber-Insurance: Towards A Unifying Framework	Böhme, R., & Schwartz, G.	2010	Theoretical cyber insurance models	https://www.researchgate.net/publication/228513115_Modeling_Cyber-Insurance_Towards_A_Unifying_Framework
54	Risk Analysis and Management	Morgan, G	1993	Overview of past risk management and analysis tools	https://www.scientificamerican.com/article/risk-analysis-and-management/

#	Title	Publisher/ Author	Date	Topic	Source
Relevant cases					
55	Sony Pictures holds USD 60 million Cyber policy with Marsh	Melissa Hillebrand	December 2014	Case analysis	http://www.propertycasualty360.com/2014/12/18/sony-pictures-holds-60-million-cyber-policy-with-m?slreturn=1491085049
56	Cyber insurance rejects claim after BitPay lost USD 1.8 million in phishing attack	Ms. Smith	September 2015	Case analysis	http://www.networkworld.com/article/2984989/security/cyber-insurance-rejects-claim-after-bitpay-lost-1-8-million-in-phishing-attack.html
57	Target credit card hack: What you need to know	Gregory Wallace	December 2013	Case analysis	http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/

The aim of this research is to provide insights into cyber insurance markets, identify future trends, and suggest areas for market developments and improvements.

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