INSTITUTE of INTERNATIONAL FINANCE

October 2019

CYBER RISK INSURANCE UPDATE:

Advances in Risk Management, Prioritizing Prevention and Protection

Mary Frances Monroe, Senior Advisor and Insurance Lead, Regulatory Affairs, mmonroe@iif.com
Martin Boer, Director, Regulatory Affairs, mboer@iif.com

INTRODUCTION

The IIF produced a staff paper on the bourgeoning cyber risk insurance market in November 2017 and found that cyber risk insurance was a growing market responding to increased demand driven by greater public awareness of cyber risk.[1] At the time, the provision of cyber risk insurance was impacted by the rapidly evolving nature of the risk, a lack of historical data, new modeling practices, legal uncertainty, and the potential for accumulation risk due to the potential interconnectedness of large cyber events. Policy makers had also begun focusing more closely on this market and how it fits into the overall regulatory and supervisory framework.

This updated staff paper will review how the cyber risk insurance market has matured since 2017, highlight the strong emphasis by insurance providers on prevention, preparation and incident response, as well as protection, and discuss innovative advances in the risk management of cyber insurance underwriting. As the market continues to grow, this Staff Report recognizes that challenges remain, including those related to "silent," or non-affirmative, cyber risk, concentration and accumulation risks, and an increase in state-sponsored attacks.

We discuss the regulatory and supervisory response to cyber risk, noting the shift in focus from resilience and reporting to the emphasis on "silent" cyber risk and sustainable underwriting practices. We offer support for the development of a common lexicon and taxonomy for cyber risk in order to facilitate further advances in risk management, as well as greater transparency and clarity around policy wordings and scope of coverage. Finally, we advance recommendations to policymakers, regulators and supervisors, including a possible role for the public sector (and/or public-private partnerships) in addressing the cyber risk insurance gap.

MARKET - Cyber risk coverage currently generates around USD 2-4 billion in annual premiums globally and is expected to grow steadily as the market matures.

PREVENTION, PREPARATION AND INCIDENT RESPONSE – Coverage increasingly includes cyber risk prevention services and post-breach response services that help both reduce the likelihood and the impact of cyber events.

CHALLENGES – As the market continues to mature there remain a number of challenges around the lack of data, "silent" risk, concentration and accumulation, as well as an increase in state-sponsored attacks.

INNOVATION – Strategic partnerships with firms in the insurtech space have been one approach to developing a team that can address the challenges of underwriting and pricing cyber insurance. However, insurtech solutions are not a substitute for robust risk management practices.

POLICY RESPONSE - The public sector can play a major role in developing a robust cyber risk insurance market by formulating appropriate, proportionate and risk-focused guidance and by supporting public-private initiatives to improve data sharing, develop a common lexicon and taxonomy, and address cyber risk insurance gaps.

[1] IIF 2017. "The emergence of cyber risk insurance: A growth market adapting to increased demand" Nov. 2017

THE MARKET FOR CYBER RISK INSURANCE

Wide range of estimates around global coverage

There is no central authority that measures the size of the global cyber insurance market, but various sources estimate it to be in the low billions of dollars. Fitch Ratings, for example, estimated in May 2019 that in 2018 the industry's total direct written cyber premiums grew 8% to USD 2 billion.[2] While noting that new premiums are slowing from 2017, Fitch still expects that high profile cyber events, the desire for more sophisticated risk management, and improved pricing will buoy the segment in the long term. These predictions for cyber insurance growth are broadly shared by other analysts but estimates vary widely. Adroit Market Research is perhaps the most optimistic, seeing the market grow to more than USD 23 billion by 2025, due to high profile cyber breaches, global regulatory developments and the fact that cyber insurance is increasingly part of corporate risk mitigation strategies.[3]

Whatever the true number, cyber risk insurance is clearly an important line of business for a growing number of insurers. In addition to covering data breaches, cyber risk insurance can also provide protection against business interruption, cyber ransom or extortion, corporate identity theft or reputational damage, depending on the scope of the policy. As will be elaborated in this report, an important element of newer forms of cyber risk coverage is the availability of cyber risk prevention, preparation and incident response services.

The range of events covered under cyber insurance policies can be broad. Cyber events can trigger multiple insurance claims, including for losses or costs incurred with respect to business interruption, data confidentiality breaches, data theft or loss, data recovery, malware, ransomware, extortion, damage to physical assets from damage to system hardware, damage to equipment from the impact of system malfunctions, customer product liability claims, directors and officers liability, errors and omissions, regulatory fines and penalties, and forensic investigations. The scope of coverage varies widely among insurance providers and individual policies. Cyber risk insurance can be provided either as a stand-alone product or as an endorsement to a more traditional policy. Industry-specific endorsements have been tailored for construction and manufacturing firms, among other sectors.

Drivers of market demand

The increasing frequency and cost of cyber events is not debatable. An October 2018 survey of around 700 UK senior managers conducted by Mactavish found that 43% of those managers reported that their company had suffered at least one cyber-attack in the prior two years.[4] Global banks have long been the prime target for cyber-attacks and see cyber-attacks as a growing concern. In an IIF survey of global banks, conducted in partnership with EY, 84% of Boards of Directors and 81% of Chief Risk Officers (CRO) deemed "Cybersecurity Risk" to be the single most important strategic priority, a significant change given that only 10% of CROs cited this risk as top of mind five years earlier.[5]

In a recent Risk.net article, it is estimated that average annual losses due to cyber events in the financial sector are between USD 38 to 100 billion per year, and that the costs of cyber events for the global economy as a whole (rather than just the financial sector) range from USD 110 to 575 billion per year.[6]

Notwithstanding the large amounts of money at stake, the overall penetration rate of cyber insurance remains low. The Association of British Insurers estimates that only 11% of U.K. companies have a specific cyber insurance policy in place.[7] The OECD estimates penetration rates of about 20%-35% in the U.S., 2%-21% in the U.K., 24% in Continental Europe and below 1% in Asia.[8] Traditionally, the cyber risk insurance market was driven by U.S. demand but, increasingly, demand is shifting to geographies outside of the U.S., partly as a result of the development of data protection standards such as the European Union's (EU) General Data Protection Regulation (GDPR), which has placed new obligations on organizations

[2] Fitch Ratings 2019. "Cyber Insurance Growth Slows, Market Remains Untested" May 14, 2019
[3] Adroit Market Research 2019. "Global Cyber Security Insurance Market Size" Dec. 19, 2018
[4] Mactavish 2018. "Cyber Risk & Insurance Report" Nov. 2018
[5] IIF and EY 2018. "Ninth annual EY/IIF global bank risk management survey" Nov. 8, 2018
[6] Risk.net 2019. "Cyber modelling masks scale of potential losses, study finds" March 27, 2019
[7] Association of British Insurers 2019. "Cyber insurance payout rates at 99%, but uptake still far too low" Aug. 8, 2019
[8] OECD 2017. "Enhancing the Role of Insurance in Cyber Risk Management" Dec. 8, 2017

and has resulted in increased cyber coverage to insure against potential GDPR fines and penalties. Recent regulatory developments in Hong Kong and Mainland China also point to a potential emerging growth market for cyber insurance. (See sidebar on page 5.)

The penetration rate for cyber risk insurance reflects predominantly large corporates; while mid-market firms increasingly have been purchasing protection, this market continues to be largely untapped. In some cases, this may be due to the perception that a cyber-attack will not impact the firm or that, even if a cyber-attack materializes, the probable losses do not warrant the cost of protection. In other cases, prospective cyber policyholders may be unclear about the scope of coverage. These perceptions point to the need for the industry and policymakers to continue outreach and education on the potential impact of cyber events. Indeed, for smaller enterprises, the existence of the company may be at stake in a cyber-attack. Insurers should also continue efforts to be more transparent and clearer about the scope of cyber coverage and to develop simpler, more standardized product offerings designed to meet the needs of mid-market firms, in line with their particular risk exposures. On the cost side, a recent trend towards cyber insurance price stabilization could alter the cost/benefit analysis for smaller firms. Some firms may face pressure from supply chain counterparties to have cyber coverage in place, which should help to boost penetration rates.

Moody's has found that the highest cyber insurance take-up rates are in the education, healthcare, communications/media/technology and hospitality/gaming sectors. Demand from health care providers in the United States has been generated by the requirements of the Health Insurance Portability and Accountability Act (HIPAA)[9]. There is an increasing demand for business interruption and ransomware cover from industrial and commercial firms that deploy robotics and internet of things devices and are concerned about the possibility of cyber-attacks that would disrupt these tools. Among financial services firms, smaller banks are becoming more cyber-aware, but one pocket of relatively low demand is among money managers and hedge funds. Take-up rates are relatively low for the financial, manufacturing, retail/wholesale and, surprisingly, the power and utilities sectors.[10] A study by the IIF on the links between cyber security and financial stability identified that attacks on the wider infrastructure – including utilities such as transport, telecoms, cable companies, and technology companies, as well as providers of data storage or cloud – could result in financial stability implications.[11] The costs of blackouts alone could be enormous. Allianz and the CRO Forum have estimated that even short blackouts that happen several times per year in the U.S. add up to an annual estimated loss of between USD 104 to 164 billion.[12]

There are limits to how much cyber cover an organization can purchase. According to Moody's, coverage of USD 25 to 100 million is now common, compared to USD 10 to 15 million a few years ago.[13] Firms can also purchase limits as high as USD 700 million through the creation of joint ventures and syndicate coverage towers. Notwithstanding the increase in coverage levels, a survey by Allianz finds that a significant majority of risk management and insurance experts believe that available cyber insurance capacity is inadequate, signaling market demand for additional coverage.[14] The OECD has noted that cyber insurance coverage limits are usually lower than limits for other perils and coverage generally is not provided for losses related to reputational damage and intellectual property theft. Traditionally, physical asset damage related to cyber events was not included in stand-alone policies, but this is increasingly covered in newer policies, as a result of offerings that were first introduced in 2013 by a Lloyd's syndicate. Stand-alone policies are closing some of the cyber coverage gaps in traditional property and casualty (P&C) policy coverage.[15]

[9] Pub.L. 104-191, 110 Stat. 1936.
[10] Moody's 2019. "Global: Battling hidden cyber exposures, insurers position for growing opportunity" July 25, 2019
[11] IIF 2017. "Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system" Sept. 2017
[12] Allianz and CRO Forum 2011. "Power Blackout Risks: Risk Management Options" Nov. 2011
[13] Moody's 2019. "Battling hidden cyber exposures, insurers position for growing opportunity" July 25, 2019
[14] Allianz 2019. "Allianz Risk Barometer" 2019
[15] OECD 2017. Op. cit.

FOCUS ON PREVENTION, PREPARATION AND INCIDENT RESPONSE

Increasingly, cyber insurance providers are offering pre-breach cyber risk prevention and preparation services and more comprehensive and timely post-breach incident response services, thus advancing the important societal goal (as well as the goal of customers) of reducing the likelihood and impact of cyber events.[16] While prevention and post-breach services are helpful additions to cyber risk insurance offerings, they are a complement to, and should not be viewed as a substitute for, policyholders' robust cyber risk management.

Prevention and preparation services reduce likelihood and impact of cyber events

Cyber risk prevention and preparation services include information security management platforms, firewalls and IP blocking technology, software security by design, training and education programs, risk and vulnerability assessments, heat maps and benchmarking (which can also be used to support underwriting and pricing), cyber risk detection systems, risk management frameworks, incident response plans, and technical assessment and monitoring programs. Prevention and preparation services can be bundled with cyber risk insurance to provide a holistic, cost-effective offering to customers. A comprehensive approach to cyber risk prevention can also help to facilitate compliance with data security standards that sometimes are a condition of coverage. Some insurers noted that policyholder utilization of cyber risk prevention and preparation services (often offered at minimal additional cost) could be improved. Greater utilization of these services would benefit policyholders and insurers alike by reducing risk.

Incident response services offered to help respond and restore

Incident response services include forensic investigations, legal counsel, data and system recovery and restoration, victim notification services, call center assistance, and crisis communications management. One major reinsurer has established a Cyber Center of Competence at the group level to examine and challenge client and market strategies for addressing and underwriting cyber risk. Another insurer emphasized the importance of policyholders having a comprehensive incident response plan in advance of any possible incident and as a condition of coverage. A third insurer offers emergency response services – such as forensic investigations and legal counsel – during the first 72 hours without a deductible in order to incent policyholders to address issues quickly and in a manner designed to control exposure.

UNDERWRITING CHALLENGES REMAIN

Addressing the lack of historical data

One of the key challenges in the modeling of cyber risk to support underwriting, pricing and risk transfer decisions, loss monitoring, and the analysis of concentration and accumulation risks arises from the sub-optimal quality of cyber loss data. Data issues stem from a number of sources, including the under-reporting and mis-reporting of cyber events, the inherent limitations of the available historical data (which is weighted toward U.S. experience), the difficulty of quantifying precisely financial losses associated with cyber events, and the decreasing relevancy of historical data in a quickly changing cyber risk environment. Deloitte analysis suggests that insurers are cautious to write cyber risk because of challenges around modeling a moving target, as new threat actors and types of attacks keep emerging.[17] However, firms report that modelling capabilities have improved considerably over the last three to four years and are becoming increasingly aligned across the major providers of cyber risk insurance.

---

[16] For purposes of this paper, we define a cyber event by reference to the CRO Forum's definition of a digital event as any incident emanating 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 use of or dependency on electronic data/systems or cyber-attack; fraud committed by misuse of data; any liability arising from data use, storage and transfer; and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies and governments. https://www.thecroforum.org/wp-content/uploads/2018/02/201802_CROF_Capture_and_sharing_of_digital_event_data.pdf.

[17] Deloitte 2019. "2019 Insurance Industry Outlook" Jan. 11, 2019

The adoption of new requirements for the prompt reporting and disclosure of cyber events (see sidebar on page 6) could help to close the reporting gap and the data could help to improve cyber risk modeling, if data transmitted to regulators could be shared on an anonymized basis with the industry, perhaps through the establishment of a private sector cyber claims repository that is supported by the official sector. New reporting and disclosure obligations could also aid in efforts to promote information sharing within and across industries on cyber threats, but the data privacy implications of information sharing must be weighed carefully. Private sector efforts to share threat intelligence and claims information are also emerging.

Another challenge is the lack of sufficient talent in cyber underwriting. One recruiter estimates that there is a "double handful" of highly talented cyber underwriters.[18] While this is most certainly an understatement of the talent in the market, our discussions with companies active in the cyber insurance market do point to a need to further develop the underwriting and actuarial talent pool.

While there are challenges to overcome, the relatively concentrated cyber risk insurance market is generally viewed to be led by mature, well-established firms with the expertise needed to manage these complex risks. As noted in this paper, insurers active in this line of business are taking a range of proactive measures designed to enhance risk management and mitigate or transfer risk. Policymakers should be attentive, however, to the possibility that less experienced players, which may be outside of the insurance regulatory perimeter, may seek to enter the market. It would make sense that firms conducting the same activities and exposed to the same risks should be subject to the same regulation.

Quantifying Cyber Losses

One of the data issues highlighted in this report stems from the difficulty that companies face in quantifying precisely the actual financial losses associated with cyber events. Financial losses can include losses or additional costs related to system downtime and remediation, and the need to hire external parties for system remediation, public relations, legal or regulatory challenges, or forensic investigations. Business interruption costs can be challenging to quantify when recovery timelines are uncertain. In addition to impacting the availability of robust historical data, the difficulties inherent in quantifying cyber losses can make it difficult for policyholders to optimize the amount and type of cyber risk cover they need.

Conducting Comprehensive Risk Assessments

A first step in mitigating the risks of cyber insurance underwriting is a comprehensive risk assessment of the prospective policyholder. Assessing the risk of a potential cyber insurance customer can be complicated by an "outside-in" approach to risk assessment, which looks at the network security perimeter without access to the data stored in the network. An "outside-in" assessment may be necessary in light of jurisdictional data privacy restrictions. Limitations on the ability to look at the risks posed by vendors – particularly downstream (vendors to vendors to a prospective customer) also can complicate underwriting and pricing decisions. To mitigate these risks, insurers are increasingly bundling cyber risk cover with tools designed to prevent a cyber-attack. For example, Zurich Insurance Group offers Cyber Risk Engineering services that identify specific cyber risks, help customers design effective remediation plans, and assist in the ongoing development and maintenance of a robust information security management system, cybersecurity strategy and related management metrics.

Apart from cyber events caused by malicious individual or government actors, cyber events may arise from the failure of a firm's employees to adhere to cyber security protocols, either deliberately or unwittingly. Assessing and predicting events arising from employee misconduct or failure to adhere to protocols can be very difficult, as they involve a risk assessment of company culture, which traditionally has not been within the purview of risk assessments conducted by insurance underwriters but is increasingly an area of focus.

[18] Financial Times 2018. Op. cit.

SIDEBAR: Cyber Risk Insurance Data Privacy and Protection Implications

An increased focus on data privacy and protection in several key jurisdictions should boost demand for cyber risk insurance. While a comprehensive catalogue of data privacy and protection laws and regulations is beyond the scope of this paper, we note that over 100 countries have implemented or are in the process of implementing some form of data privacy and protection legislation. [19]

In the EU, the GDPR Framework came into effect in June 2018. The GDPR applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) or the monitoring of behavior that takes place within the EU.

Under the GDPR, a data controller generally is required to report a data breach to the appropriate supervisory authority within 72 hours. Data processors are also required to notify data controllers without undue delay upon becoming aware of a data breach. Organizations in violation of the GDPR can be fined up to 4% of annual global turnover or EUR 20 Million (whichever is greater).

The U.S. does not have a single data privacy and protection legislative framework at the federal level, nor is there one regulatory body responsible for data privacy and protection. Rather, data privacy and protection requirements are sector-specific, specific to the source or type of data processed, or state-specific. As a general matter, the U.S. Federal Trade Commission (FTC) can bring enforcement actions to protect consumers against unfair or deceptive practices and this authority has been interpreted as including the FTC's ability to address the failure of a company to adhere to its own data privacy and protection policies or to adequately safeguard customer information. Data privacy and protection requirements are also contained in various federal laws, including HIPAA, the Fair Credit Reporting Act (15 USC 1681), and the Gramm-Leach-Bliley Act (15 USC 6802(a) *et seq*. Some states have adopted data privacy and protection legislation, notably, the Commonwealth of Massachusetts and the State of California.
Each of the U.S. states and territories has adopted cyber event reporting and notification requirements but the requirements vary considerably from state to state. The National Association of Insurance Commissioners has adopted an Insurance Data Security Model Law, based generally on the regulations of the New York Department of Financial Services (NYDFS), which provides for reporting a cybersecurity event within 72 hours to the regulators and providing notice to consumers in a manner and on a timetable consistent with state law. To date, South Carolina, Ohio and Michigan have adopted the new model law.

New York State has had cybersecurity regulation since 2018 for financial services companies; the regulations include requirements for a cybersecurity program and policies, an incident response plan, the designation of a chief information security officer, the establishment and maintenance of a cybersecurity event reporting system, at least annual penetration testing and bi-annual vulnerability assessments. Effective in 2019, companies must also establish policies to manage the cyber risk of vendors and suppliers. Companies are required to submit to the NYDFS an annual attestation of compliance with the regulations, signed by a senior officer or the board of directors.
The Hong Kong Insurance Authority (HKIA) issued guidance on cybersecurity in June 2019 that was influenced by the NYDFS regulations. While cyber risk insurance is not yet widespread in Hong Kong, the HKIA is expected to participate in industry discussions regarding the provision of cyber risk insurance.

Recent developments also point to an emerging market for cyber risk insurance in Mainland China. Recent reports note that the Chinese authorities are increasing their focus on cybersecurity incidents and consumer data protection practices. New regulations have been established for cloud services suppliers to Communist Party or government agencies, or to critical information infrastructure operators.[20] The Cloud Computing Service Security Assessment Measures emphasize, among other elements, the feasibility and convenience of customer data portability.

[19] Moody's (2019), op cit.
[20] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-security-reviews-cloud-services/

Speaking to "Silent" Risk

A significant issue, both for cyber insurance underwriting and cyber resilience, is the exposure to "silent" or, more accurately, non-affirmative cyber insurance risk. Non-affirmative cyber insurance is silence in an insurance policy regarding the treatment of cyber-induced physical and/or non-physical loss.

One example of non-affirmative cyber insurance risk would be a cyber-attack on a manufacturer that would cause a fire to damage its robotic equipment. Even without a specific endorsement covering cyber events, an insured may claim that a general P&C insurance policy covers a cyber event and, if litigated, a court may side with the insured plaintiff. General exclusions may not provide adequate protection against these risks. Given that P&C exposure limits are many multiples of the coverage limits for cyber risk, the exposure to non-affirmative cyber risk is significant. Insured losses from one event alone, the Petya/NotPetya attack, are estimated at USD 3.3 billion, with up to 90 percent attributed to non-affirmative cyber risk.[21]

To proactively address so-called "silent" cyber risk and related legal and litigation risks, insurers are transitioning to affirmative cyber coverage,[22] implementing exclusions or sub-limits in traditional P&C policies, reviewing and revising legacy contracts, and drafting new contracts that provide greater clarity with respect to contract terms and exclusions. Companies are taking different approaches to addressing the scope of coverage issues related to non-affirmative cyber risk. Some are covering physical damage and bodily injury arising from cyber-attacks (and the related business interruption losses) under traditional P&C policies but requiring affirmative contracts to cover financial losses without physical damage or bodily injury. Others are adding endorsements to existing policies to cover business interruption or other specific consequences from cyber events and adding cyber event definitions to updated policy wording. (While non-affirmative cyber risk generally arises under traditional P&C policies, there is also a need to confirm whether cyber events are covered under specialty insurance products, such as those insuring risks related to aviation and marine.)

Concentration and Accumulation

Cyber risk policies are particularly susceptible to concentration and accumulation risks. Accumulation risks from a single cyber event can have a global reach and, thus, cyber accumulation risk can be much more significant than accumulation risk that arises in other more localized lines of business. The widespread use of cloud computing services provided by a limited number of cloud service providers (CSP) could give rise to concentration and accumulation risk if a cyber-attack were to compromise a CSP. Concentration and accumulation risk could also arise from exposure to a common vulnerability such as a widely-used operating system.

Estimates of loss from a massive attack vary widely, pointing to the difficulty insurers face in pricing for concentration and accumulation risk. Accumulation models are under development by insurers with expertise in underwriting natural catastrophe risk, as well as by new insurtech firms entering the market. Models include both traditional deterministic and probabilistic models and algorithm-driven models. Insurers and vendors are working on ways to improve the quality, rigor and objectivity of accumulation models. The industry's move from non-affirmative to affirmative cyber cover will also help address concentration and accumulation risks.

State-Sponsored attacks

Cyber threats from government or government-sponsored actors are an increasing concern to insurers, as the number and level of sophistication of these attacks has increased. Insurers are refining their approaches to the standard insurance "war exclusion" to consider how to define and address cyber-attacks that may be considered acts of war. Some insurers are differentiating attacks based on whether they facilitate or lead to physical damage or bodily injury. Others consider acts of war to encompass disruption to critical infrastructure, whether tangible (brick and mortar) or intangible. A complicating factor is the difficulty of attributing a cyber-attack to a state (or state-sponsored) actor, which generally requires a lengthy and costly forensic investigation. Attribution can be critical to determining whether an event is insured.

[21] Allianz 2019. Op. cit.

[22] For example, AIG has announced that it is transitioning to affirmative cyber coverage by January 2020.

Cyber Risk Transfer

To transfer the risks of providing cyber insurance cover, insurers generally access the reinsurance market. To date, the alternative risk transfer market (e.g. cyber risk bonds, insurance-linked securities) has not covered these risks but this could be a potential future development. Investor interest in cyber risk is said to be low given limited understanding of the risk and interest in time-limited exposure. The direct insurers and reinsurers we surveyed believe that current reinsurance capacity is sufficient to accommodate existing demand without alternative sources of risk transfer, but this could change in the event of a material uptick in demand or a significant accumulation event.

INNOVATIVE ADVANCES

How "insurtech" is supporting Risk Management approaches

Strategic partnerships with firms in the insurtech space have been one approach to developing a team that can address the challenges of underwriting and pricing cyber insurance. As cyber risk has evolved, and the difficulty of quantifying its potential impact has increased, specialized insurtech firms have developed various modeling techniques to help insurers and their clients more accurately assess their cyber exposures. While these solutions can augment an insurer's underwriting and pricing capabilities, they are not a substitute for robust risk management and a well-managed and controlled underwriting and pricing approach. It is also important for an insurer to conduct an appropriate level of due diligence prior to using insurtech solutions in order to ensure that the data sources used in algorithms and models are robust and up to date.

The following descriptions of insurtech innovations are based on publicly available information from company websites:

Bitsight and SecurityScorecard provide insurers with algorithmically derived security ratings for current and prospective policyholders, based on externally available data, along with comparisons to industry benchmarks. These security ratings and benchmarks can augment an insurer's underwriting capabilities.

Risk Management Solutions (RMS) and AIR Worldwide (AIR) are two organizations offering cyber risk solutions to insurers through their probabilistic cyber models. 'V3 Cyber Model', the model released by RMS in 2018, provides insurers with the ability to capture standardized cyber exposure data and to perform risk modeling against a range of cyber loss events. RMS has created a series of models to determine plausible examples of system cyber catastrophes in order to support risk selection, underwriting decision-making and technical pricing. In 2018, AIR developed its own probabilistic model for cyber risk, which is capable of estimating the likelihood, severity, and economic and insurance impact of security breaches and CSP downtime incidents.

CyberCube provides tools to model the cyber risk landscape, allowing users the ability to configure frequency and severity controls to create a bespoke view of risk and manage tail risk by optimizing pricing and reinsurance decisions. CyberCube's tools also allow users to benchmark their cyber risk exposure against peers and analyze trends.

Guidewire's Cyence Risk Analytics (Cyence) platform collects, curates and analyzes technical and behavioral data to build cyber risk modelling solutions that provide fact-based measures of probable maximum loss. Cyence recently developed a scenario designed to estimate the origin of losses due to a mass business interruption following a ransomware event.

Corax is a cyber risk modelling and prediction platform that leverages proprietary data on the cyber resilience of several million companies to provide insurers with benchmarking, predictions and probabilistic expected loss estimates. Platforms such as those provided by Corax can help insurers with underwriting and managing cyber risk.

In addition to the services offered to insurers, various risk services are offered directly to policyholders by insurtech firms. For example, Aida, provided by Socure, is a patented identity verification bot which continuously sources live digital data, using machine learning to create a holistic customer identity model. Cyber Risk Global Exchange offers policyholders the ability to develop an inventory of third-party vendors, enabling them to more accurately assess the risks presented through their portfolio of business relationships. Risk services are also offered to policyholders by insurers that have developed in-house expertise and proprietary models.

REGULATORY AND SUPERVISORY RESPONSES

Increasing awareness around the importance of cyber insurance coverage

Historically, the regulatory and supervisory response to cyber risk focused on the resilience of the insurance sector to cyber risk attacks. Lately, the focus has shifted to a consideration of the risks of providing cyber risk coverage.

The regulatory and supervisory community has increased its awareness of the important societal benefit provided by the availability of cyber risk cover, while also considering the risk management challenges of this market and the need for guidance to address these challenges. The supervisory response to date has varied across jurisdictions, with varying levels of attention to the issue. The Bank of England Prudential Regulatory Authority (PRA) has been particularly active in the area of cyber risk. The PRA published the results of a survey on cyber underwriting risk in January 2019[23] and has since directed insurers under its jurisdiction to take concrete steps to address "silent" cyber risks. (Lloyds has followed suit, directing insurers in its syndicates to provide clarity on cyber risk coverage in first-party contracts by January 1, 2020.) BaFin has also indicated that it will pay particular attention to "silent" cyber risk.

Key IAIS focus on promoting sustainable cyber underwriting

The International Association of Insurance Supervisors (IAIS) has announced the formation of a new working group to assess the role of insurance supervisors in promoting sustainable cyber underwriting, looking at potential risks and impediments to sustainable cyber risk underwriting, such as accumulation risk, non-affirmative cyber cover, standardization of terminology and coverage and modelling gaps due to lack of data. The IAIS previously published an August 2016 Issues Paper and a November 2018 Application Paper that addresses insurers' cyber resilience[24]; the focus is now shifting to the provision of cyber cover. In the June 2019 IAIS Newsletter, IAIS Secretary General Jonathan Dixon noted:

> "Trends and developments such as FinTech, cyber risk, climate risk, and the challenge of sustainable development, will reshape the business of insurance in the coming years. As the global community of insurance supervisors, the IAIS will support our Members in proactively responding to these challenges and opportunities."

We applaud the efforts of insurance regulators and global standard setters to understand both the challenges and opportunities of this line of business and to appreciate the important social benefits that are provided by cyber risk insurance. We encourage further dialogue among policymakers, the industry, academics and other informed parties in order to promote a collective understanding of the challenges and opportunities of cyber risk insurance and a coordinated regulatory and supervisory response that facilitates a level playing field.

Given the rapidly changing nature of the market and of the risks, we would encourage a regulatory and supervisory approach that favors principles and outcomes over prescription. A prescriptive approach could become outdated very quickly in a fast-moving environment and could stifle much-needed innovation and hinder the development of bespoke products and services for customers with a range of coverage needs. Regulators should work to develop common standards and guidance in order to minimize regulatory fragmentation and burden on insurers operating across multiple jurisdictions and to promote a level playing field.

Policymakers could also serve an important role in educating companies and individuals about the need for robust cyber risk management and preparedness. Part of this effort could include promoting a legislative framework that holds businesses responsible for adopting appropriate cyber security measures.

Value of a Common Lexicon and Taxonomy

At present, a variety of lexicons are used to define cyber risk and various taxonomies exist or are in development to describe and categorize cyber threat information. Some of these lexicons and taxonomies are very technical and developed for specific uses or for particular sectors or sub-sectors (e.g. aviation or marine). The types of events captured may vary

[23] Bank of England 2019. "Cyber underwriting risk: follow-up survey results" Jan. 30, 2019
[24] IAIS 2018. "Application Paper on Supervision of Insurer Cybersecurity" Nov. 2018

across taxonomies (e.g. some capture relatively minor breaches of information technology security while others capture only material cyber risk events that require reporting to a regulator), reflecting the purpose for the taxonomy (e.g. as a preventative tool or as a tool to analyze losses).

A number of commentators have advocated in favor of the development of a common general cyber risk lexicon and taxonomy that could be used more broadly.[25] A common lexicon and taxonomy, developed jointly by the industry and the regulatory and supervisory community, could support cyber insurance underwriting and pricing by providing a framework for categorizing cyber event data along several dimensions, including incident types, affected data, financial/business impact, root cause, and actor. Quantifying the financial impact or loss along these dimensions could enable cyber insurance underwriters to sharpen and better differentiate their pricing of risks and improve risk management. A common lexicon also could facilitate transparency and clarity around policy terms and conditions, encourage more reinsurance capacity (and perhaps help in the development of an alternative risk transfer market), and allow for a better comparison of cyber coverage offerings by prospective policyholders. It may still be necessary to develop more detailed, bespoke lexicons and taxonomies for specific sectors, but a common standard lexicon and taxonomy would go far in reducing the confusion created by multiple competing approaches.

Support for a common lexicon and taxonomy is not universal, however. Other commentators have raised concerns that a common lexicon could stifle innovation and the development of the cyber insurance market. The market is relatively young and the definitions of triggering events and categories of losses continue to evolve. As such, there is concern that static definitions in a taxonomy could inhibit market development and innovation.

Developing a public sector backstop

Some of the companies we interviewed in the process of writing this report see a role for the public sector in providing or backstopping cyber risk cover. One company noted that current capacity is sufficient but, if demand grows, that capacity could be quickly overwhelmed. A particular need for additional cyber cover may arise from the growth of personal lines and coverage of mid-market and smaller enterprises.

Other companies noted a need for a fair sharing of the risks among direct insurers, reinsurers, and governments, particularly in cases of cyber terrorism or acts of war and in response to accumulation risk. There may be an opportunity for public sector involvement to address the fact that there are few clear cases of attribution; government resources and data could be used, perhaps in coordination with IT professionals and academics, to enhance the ability to trace cyber incidents to their sources.

Other potential roles for the public sector include the development of a cyber incident database. A model for this could be the U.S. Financial and Banking Information Infrastructure Committee, a public sector organization with a focus on cyber security that was designed to improve coordination and communication among financial regulators and to promote public/private partnerships, including joint efforts with the private sector. The U.S. Financial Services Information Sharing and Analysis Center is an industry consortium with a mission to anticipate, mitigate and respond to cyber threats. The development of a repository would be successful in mitigating cyber threats only if firms are willing and able to contribute comprehensive information.

[25] Brookings 2018. "The future of financial stability and cyber risk" Oct. 10, 2018

RECOMMENDATIONS FOR POLICY MAKERS, REGULATORS AND SUPERVISORS

We would offer the following recommendations to policymakers, regulators and supervisors charged with developing guidance for insurers providing cyber risk cover:

- Policymakers, regulators and supervisors should continue their efforts to better understand cyber risk, the market for cyber risk insurance, and advances in insurers' risk management and governance through dialogue with providers of cyber risk cover and reinsurance, academics and experts in risk management and modeling, and other public sector authorities.

- Policymakers, regulators and supervisors should expand educational efforts to their peers in markets where cyber risk insurance may be in the early stages of development.

- Policymakers, regulators and supervisors should promote robust cyber risk management and engage in educational initiatives designed to improve cyber security awareness and readiness.

- Policymakers, regulators and supervisors can help the industry promote the utilization of cyber risk prevention services as a complement to robust cyber risk management in reducing the likelihood and impact of cyber events.

- Policymakers, regulators and supervisors should work with the industry and other stakeholders to develop convergence around appropriate regulatory and supervisory standards. Flexible, non-prescriptive guidance that reflects the rapidly evolving market for cyber risk insurance and the commitment of market participants to sound underwriting of these complex risks should be applied in a proportionate and risk-focused manner.

- Regulators should seek convergence in cyber risk regulations and guidance across jurisdictions, across all firms conducting cyber risk insurance activities, and across the financial services sector to the extent appropriate and practicable. Consideration should be given to basing regulations and guidance on established industry standards, such as the U.S. National Institute of Standards and Technology Cybersecurity Framework.

- Policymakers, regulators and supervisors should promote the development of a common standard lexicon and taxonomy for cyber risk with involvement from both the industry and public sector.

- Public sector authorities should promote the private sector provision of appropriate and affordable cyber risk cover to mid-market and smaller enterprises and individuals.

- Public sector authorities should consider the feasibility of a government or multilateral backstop arrangement that would become operational in the event that a severe accumulation risk event or state-sponsored attack materializes.

- Public sector authorities should continue to enhance efforts to attribute cyber incidents to their sources.

- Public sector authorities should partner with insurers to identify solutions that encourage and support the sharing of incident data in a timely, complete and accurate manner.