Chapter 5

Addressing challenges to cyber insurability

This chapter examines ways to address the challenges that impede the development of the cyber insurance market. The development of probabilistic models for cyber risk could improve underwriting and reduce uncertainty although this will require improved data on past incidents and their impact as well as on the relative effectiveness of security policies and practices. There are several potential sources of data that could support probabilistic modelling and a few initiatives aimed at sharing this data within the insurance sector and between the government and the private sector. However, a lack of harmonisation limits the contribution of these efforts. The insurance sector and governments in several countries are also examining ways to improve understanding of the insurance coverage available for cyber risk and at least one country has implemented a regulatory intervention to encourage greater transparency.

A number of initiatives are being established to help address the various challenges to the development of the cyber insurance market by governments, the insurance industry and through public-private cooperation. This chapter provides an overview of the initiatives focused on two critical issues for the further development of the market: (i) improving the capacity to quantify cyber risk; and (ii) addressing the challenges in understanding cyber insurance coverage. This is followed by a short discussion of other approaches that could support the development of further market capacity.

Improving the capacity to quantify cyber risk

As outlined in Chapter 4, the limited availability of data on past cyber incidents, the rapid pace of change in the nature of cyber risk, uncertainty about the effectiveness of different security technologies in terms of risk reduction, and the potential for accumulated losses have a negative impact on the supply of insurance coverage for cyber risk and lead to higher premiums for the coverage offered. In the case of other perils, such as natural hazards and terrorism, the development of models has made an important contribution to reducing uncertainty and managing accumulation risk, ultimately improving market efficiency (see Box 5.1).
Box 5.1. The modelling of natural hazard and terrorism risk

While there are a number of important differences in the nature of these risks, the development and use of data and modelling infrastructure to support the underwriting of insurance coverage for natural hazards and terrorism (as well as the management of the exposure transferred to reinsurance and capital markets) could provide lessons for the cyber insurance market.

Modelling of natural catastrophe risks began in the late 1980s (Swiss Re, 2017b) and accelerated in the aftermath of Hurricane Andrew in 1992 as a result of large (unexpected) losses across the insurance sector that clearly demonstrated the significant gap in the understanding of exposures to hurricanes (and other natural perils). Natural catastrophe models use data on hazards and their physical parameters (wind speed, ground-shaking), assets-at-risk (i.e. buildings and infrastructure), damage functions (i.e. the likely level of damage that would result from the impact of a given physical parameter, such as wind speed or water level/velocity) and insurance coverage to provide estimates of insured exposure for a range of natural perils. These models incorporate estimates of the probability of a broad-range of different events occurring, allowing for an insurer to estimate their annual average loss and their probable maximum loss for a given return period. These estimates are used for underwriting (and pricing) insurance coverage, transferring risks to reinsurance and capital markets and for the calculation of capital requirements.

The first probabilistic models for terrorism risk were developed following the September 11th terrorist attacks in the United States (which also led to significant unexpected losses across the re/insurance sector). These models provide estimates of frequency using an inventory of potential targets (based on symbolic or economic significance) and the relative likelihood of different attacks based on the complexity of preparing the attack and the probability of success (including a suppression factor based on an assessment of government's ability to prevent such attacks) (Risk Management Solutions, 2014).

The development of these models has benefitted greatly from several external sources of data and analysis, including: (i) decades of trusted data on the occurrence of natural hazard events and their physical characteristics from government meteorological, geological and hydrological institutions and on terrorism events (and unsuccessful plots) from specialised tracking institutes; (ii) for natural hazards, a real-time monitoring infrastructure for many types of natural perils, such as weather stations, satellite imagery, seismographs and river gauges); (iii) extensive databases on buildings and infrastructure (and landmark buildings and infrastructure); (iv) engineering studies on the impact of physical parameters such as wind speed, water height or explosions on structures; (v) years of (often harmonised) claims data, including through claims data aggregators, to support the calibration and verification of models; and (vi) extensive scientific analysis of natural hazard and terrorism risks and their evolution which allows model developers to leverage scientific advancement in understanding these risks (one of the main advantages of models is that they make use of both historical experience and expert understanding of the nature of the peril to develop estimates (Marsh & MacLennan, 2016)).

While these models cannot provide perfectly accurate estimates of the probability of a given event or the precise impact of an event with specific characteristics, regular advancements have led to a level of convergence across different commercial models (suggesting reduced uncertainty) and increasing confidence in the estimates that they generate (Swiss Re, 2017; Hancock, 2017).

Currently, modelling of cyber risk is mostly scenario-based - providing a framework for deterministic estimates of losses - although without providing a basis for estimating the probability that the given scenario might occur (Swiss Re, 2017). As existing scenario-based models have been focused on extreme incidents (including incidents involving a high potential for correlated losses), they are mostly being used for managing accumulation risk rather than for pricing. Two of the major commercial modelling firms (AIR Worldwide and Risk Management Solutions (RMS)), for example, have developed extensive data sets that allow for calculations of potential losses at different companies under a diverse range of scenarios (Swiss Re, 2017). Similarly, Lloyd's has developed a
Realistic Disaster Scenario for a major data security breach based on a common system or software vulnerability and has committed to developing ten more scenarios to assist syndicates' analysis of potential losses from various types of incidents (Lloyd's, 2016a; Lloyd's, 2016b). However, the (fortunate) scarcity of extreme incidents limits the ability to attach frequency estimates to these scenarios (or even to most less-extreme scenarios) (Swiss Re, 2017). Some probabilistic models have been developed for higher-frequency incident types such as third party (personal) data confidentiality breaches given the greater availability of data. There are also a number of new entrants that are developing different approaches to adding a probability component to existing models, including through the use of cyber value-at-risk models (Swiss Re, 2017).

The following sections will examine initiatives that could help address the dearth of data on incidents, accumulation risk and the effectiveness of protection measures which, if overcome, could support the development of probabilistic models of cyber exposure over time (although it took many generations of catastrophe models before the necessary level of precision for building wider trust and acceptance was achieved (Fitch Ratings, 2017)).

**Incident data sharing initiatives**

A critical requirement for developing probabilistic models is availability of sufficient data to predict with some confidence the probability distribution of incidents of varying severity (i.e. not just the impacts of specific scenarios but the probability that such an event could occur within a given return period). As noted in Box 5.2, natural hazard models achieve this through analyses of (extensive) historical data as well as from the findings of scientific research into the nature of the perils (including any potential for changes in frequency and severity) – none of which is readily available in the case of cyber risk.

There are a number of sources of information on cyber incidents in government and in the private sector:

- **Government sources of information on cyber incidents:** Within governments, the main sources of information on cyber incidents are computer security incident response teams (CSIRTs, also known as computer emergency response teams or CERTs), privacy enforcement authorities and sectoral regulators. Governments (e.g. responsible line ministries or national statistical offices) may also collect information through business surveys, either regularly or periodically (see OECD, forthcoming). CSIRTs have been established in a number of countries in order to “prevent, handle and mitigate computer security incidents” (OECD, 2013). CSIRTs collect technical data on incidents that they handle and many use that data to generate (and often publish) statistics on trends in the types of cyber incidents (OECD, 2013) (although with a potential for bias based on the type of incidents that are reported to CSIRTs).

Privacy enforcement authorities collect data on data confidentiality breaches involving personal information that are reported to them based on applicable notification requirements. Many of these authorities will publish annual statistics on the number of breaches and the number of records exposed (among other indicators). As noted above, the volume of incidents that will be reported to privacy enforcement authorities is expected to increase as a result of the spread of reporting and notification requirements around the world, which means that these authorities are likely to have a more comprehensive picture of these types of incidents in the future (see Box 2.2). For example, national supervisory
authorities responsible for the implementation of the GDPR in the EU will be required to prepare annual reports which may include information on the types of incidents that led to privacy infringements.

Sectoral regulators, such as financial or energy sector regulators, may require the companies that they regulate to notify them of any (or any material) cyber incidents. For example, almost all responses to the OECD questionnaire from insurance regulators indicated an expectation that insurance companies would notify their supervisors of an incident and some had specific requirements for notifying supervisors of material incidents. In some cases, the relevant regulator will publish aggregated information on the incidents reported to them although this occurs much less frequently than in the case of CSIRTs or privacy enforcement authorities. In addition, regulators (whether sectoral or functional) could also impose requirements for the disclosure of cyber incidents (e.g. the US SEC disclosure requirements).

Finally, many insurance regulators (or statistical agencies) collect and publish data on premiums written and claims paid for different business lines by the insurance companies that they oversee. However, at the time of writing, only the US National Association of Insurance Commissioners indicated that they collected regular data on stand-alone cyber insurance premiums and claims (many others collect such data only as needed). Such information would provide statistics on the aggregate value of the insurance payments made, although not specific information on the types of incidents or their individual impacts.

Data and statistics provided by government agencies is rarely harmonised across countries (or even across agencies, given the different drivers behind the data collection). In 2013, the OECD (2013) developed guidance for improving the comparability of statistics provided by CSIRTs. The OECD has also recently begun an assessment of the comparability across countries of personal data breach notification reporting which could lead to greater consistency in terms of the resulting statistics. There is little known information sharing on incidents across sectoral regulators (or efforts to harmonise approaches). The G7 has established a Cyber Expert Group to share information and practices related to cyber security among financial sector regulators although no work on harmonising incident reporting is being planned by this group. The European Union Agency for Network and Information Security (ENISA) intends to examine how mandatory incident reporting schemes within the European Union (e.g. GDPR and NIS directives) could be harnessed as a source of useful incident data for insurance companies.

### Private sector sources of information on cyber incidents

Individual insurance companies collect information on incidents affecting their policyholders (where a claim is made) although this information is usually not publicly available (outside of the initiatives described below). In addition, there are a number of private sector companies and organisations that collect data on incidents as a service (or as input into a service) provided to the insurance industry. One US-based company (Advisen) has reportedly collected information from public sources (media reports, legal analyses, freedom of information requests) on more than 35,000 data confidentiality breaches, data integrity/availability incidents, system malfunctions and malicious activities (Advisen, 2017). There are also at least three major databases that provide information on operational risk incidents,
including cyber incidents. One dataset (SAS OpRisk Global Data) is based on publicly available data and reportedly includes over 25 000 operational incidents since 1995, including cyber incidents (Eling and Wirfs, 2016). The ORX database includes an anonymised set of incidents reported by its financial sector members from around the world (although this data is not publicly available). ORIC, a membership-based organisation for insurance and asset management companies, also provides a platform for sharing information on operational risk incidents. Commercial modelling companies, such as RMS and AIR Worldwide, also collect extensive information (including from third-party commercial sources) on cyber incidents in order to calibrate their models.

There are a number of efforts to harmonise claims and incident data in the insurance sector. Lloyd’s has established common coding for reporting data on cyber insurance coverage provided by Lloyd’s syndicates, including a code for cyber security data and privacy breach (CY)² and a code for cyber security property damage (CZ)³ (Lloyd’s, 2015). Two of the major modelling firms (AIR Worldwide and RMS) have released data categorisation schemas in order to encourage the collection of harmonised data on company characteristics, risk management practices, incidents and loss types. The two modelling companies and Lloyd’s have also agreed on a set of common core data requirements (Lloyd’s, 2016c) (see Table 5.1).

There is also at least one initiative aimed at collecting a harmonised set of incident data. Since January 2017, the ORX database is receiving cyber incident reports from insurance companies on a pilot basis using the CRO Forum data categorisation (which is also used in this report) (Bishop, 2017). The pilot exercise involves reporting by members on incidents that have affected their own systems only (not those affecting their policyholders). There are also a few initiatives aimed at collecting claims information on a harmonised basis. One organisation, NetDiligence, has been publishing cost of claims studies for a number of years. It’s most recent study (NetDiligence, 2016) included claims data from 17 insurance companies operating in the US market, including a number of the largest providers, and appears to cover a significant (50% to 70%) share of claims paid in the US market.⁴ One of the two main aggregators of insurance claims data for natural catastrophe events,⁵ the Insurance Services Officer (ISO), undertook a cyber insurance data call to collect premium and loss data for cyber liability and first-party coverages written between 2010 and 2014 (based on the AIR Worldwide categorisation) and has also launched a platform for aggregating losses related to large cyber incidents (see Box 5.5).

A number of information sharing initiatives have been established by - or between - governments and the private sector, although most are focused on sharing operational threat information rather than incident reports (see Box 5.2). In the United States, the Department of Homeland Security has established a Cyber Incident Data and Analysis Working Group which is working on the development of a Cyber Incident Data and Analysis Repository. The objective of the repository is to provide standardised data on past incidents that would allow for the risk analysis necessary to support "better cyber risk assessments, enhanced cyber incident modelling and prediction, and more cost-effective and dynamic cybersecurity programs" (Department of Homeland Security, 2015). An initial set of potential data categories were published for consultation in September 2015 and included categories for company characteristics, type and severity of incident, risk management approaches and impacts and costs (among others) (see Table 5.1).
Box 5.2. Public-private threat information sharing initiatives: selected examples

A number of countries have established mechanisms for sharing information on operational threats between the public and private sectors:

- In the United States, a number of Information Sharing and Analysis Centers (ISACs) have been established for critical infrastructure sectors as trusted environments for sharing threat information (supported by specific legislation to protect against liability and other risks of data sharing). While the ISACs have been established to address multiple risks, some of the sectoral ISACs (such as the Financial Services ISAC (FS-ISAC)) focus extensively on sharing operational and technical information related to cyber threats, including both information identified by private sector members as well as by government. Some, such as FS-ISAC, also operate internationally.

- In the United Kingdom, a Cyber Security Information Sharing Partnership has been established to exchange cyber threat information, including threat analysis provided by a “fusion cell” analytical team comprised of government and industry experts, as well as alerts and threat advisories, weekly and monthly summaries and a malware and phishing email analysis service. The service is free and open to both businesses and individuals.

- In Switzerland, the “Reporting and Analysis Centre for Information Assurance” (MELANI, its acronym in German) provides threat and mitigation information to both individuals and businesses. It also provides a more comprehensive service for operators of critical infrastructure, bringing together the intelligence available through law enforcement, security and intelligence agencies as well as computer emergency response teams.

- In Canada, the Canadian Cyber Threat Exchange has been established as a not-for-profit organisation to share information on cyber threats and vulnerabilities among businesses, government agencies and research institutes. It provides various levels of services to its members, ranging from direct access to its analysts and access to closed information sharing platforms to advice available to the general public on how to protect against identity theft and fraud.

- In France, “Action against cyber crime” (ACYMA, its acronym in French) was established in 2015 as a national platform with three objectives: (i) providing victims (businesses, individuals and local governments) with access to expert advice; (ii) organising awareness and prevention campaigns; and (iii) creating an observatory of digital risks that will support predictive analysis of threats.

These initiatives have generally been established with the aim of preventing cyber incidents and therefore do not provide a platform for sharing information on incidents that have occurred. However, the information that is collected on threats could potentially prove useful for understanding the evolution of cyber incidents. It could also provide a source of data on attempted attacks and success rates - which might both prove useful for probabilistic modelling of cyber risk (as is the case for modelling terrorism risk).

Table 5.1 provides an overview of the types of incident data that are collected (or recommended for collection), as well as the specific data categories (where available) across a few of the major data aggregation initiatives (US Cyber Incident Data and Analysis Working Group, Advisen, CRO Forum, AIR Worldwide and Cambridge Centre for Risk Studies). Four of the five initiatives include a specific categorisation of cyber incidents, although there is currently no harmonisation in terms of incident categories across initiatives, with a wide variety of different categories used as well as differences in terms of the scope of incidents covered. All of the initiatives include a categorisation of impacts, including non-financial indicators of impact in the case of two initiatives (US Cyber Incident Data and Analysis Working Group and Advisen). The CRO Forum and Cambridge Centre for Risk Studies' classifications of financial impacts (types of losses) are closely harmonised and can be mapped to the AIR cyber exposure data standard. The
US Cyber Incident Data and Analysis Working Group classification plans to include a much more granular classification of some types of impacts (e.g. incident response costs) and a much less granular classification of others (e.g. liability). The US Cyber Incident Data and Analysis Working Group also intends to collect data on a variety of incident attributes (detection time, attacker motivation, specific control failures, etc.) not collected in the other initiatives.

While a lack of harmonisation across these initiatives limits the availability of comparable data for use in developing probabilistic models of cyber risk, there are also a number of factors that limit the amount of data shared by participants within these initiatives. Sharing of incident data within the insurance industry and between the public and private sectors could be limited by concerns related to: (i) the robustness of the "anonymisation" process, which requires that an appropriate balance be found between providing a sufficient level of detail on incidents without allowing for the identification of the affected organisations; (ii) strength of the security controls protecting the repository, including ensuring sufficient security amongst those able to access the repository; and (iii) confidence in the neutrality and independence of the organisation responsible for the repository, given the need to ensure that data is managed, processed and used appropriately.

From the perspective of insurance companies, there may also be more significant obstacles to disclosing information on incidents that affected their policyholders (relative to incidents that affected the insurance companies themselves (American Insurance Association, 2016)) - notably the potential for liability or for disclosing information that may be subject to future litigation. Insurance companies that have built-up significant claims experience may also be reluctant to share that experience with other companies for competitive reasons (as claims experience can provide a competitive advantage in terms of underwriting). However, one recent global survey found a relatively high-level of acceptance (68% of respondents) that data and information sharing on cyber risk will increase. Close to half of all respondents across most industries indicated that they were prepared to collaborate more strongly in terms of information sharing on an industry-wide basis and with insurance companies (particularly in the hotel, industrial products, consumer products and chemical and petroleum sectors although the media, healthcare and transportations sectors indicated less willingness to collaborate) (Swiss Re, 2016; Swiss Re, 2017).

Access to threat information from government might also provide an incentive for joining information sharing initiatives more generally (Marsh & McLennan Companies, 2016), as could encouragement from regulators. For example, the US National Association of Insurance Commissioners indicated that it encourages the insurers it regulates to share information on incidents in order to improve the collective knowledge of cyber threats.

The establishment of information sharing initiatives also faces practical obstacles that must be overcome, such as what type of organisation is best-placed to host an incident repository. Some of the threat information sharing initiatives (e.g. US Information Sharing and Analysis Centers, Canadian Cyber Threat Exchange) have been established as membership-based not-for-profit organisations while others (e.g. Melani, ACYMA) are government or government-sponsored agencies. The US Cyber Incident Data and Analysis Working Group has not identified a host organisation for the proposed incident repository (although it is not recommending that the repository be hosted by the government). Some insurance industry initiatives (ORX and ORIC International) are
membership-based organisations established for the specific purpose of providing data and analysis to contributing members. Others, including NetDiligence, Advisen and the Insurance Services Office, are independent, for-profit service providers that have been established to specifically offer services to other companies (cyber security assessment services in the case of NetDiligence and a range of insurance-related services in the case of Advisen and ISO). The for-profit organisations could be driven by competitive pressures to develop broader and better data coverage, although competition between them could lead to the development of proprietary arrangements and other practices that would prevent the establishment of a comprehensive repository.

**Data on the effectiveness of risk management approaches**

As noted above, the quantification of cyber risk exposure also requires an assessment of the relative effectiveness of risk management processes and technologies in both reducing the probability of an incident and the impact of incidents that do occur. While not only a challenge in the case of cyber risk (for example, see OECD (2016) for a discussion on the challenges in measuring and recognizing the effectiveness of flood protection measures), the wide variety of available cyber security technologies makes this particularly challenging in underwriting coverage for cyber risk. One estimate has suggested that there are more than 600 products on the market for protecting digital assets and that some large organisations might use more than 100 of these products in their cyber risk management (Harrington, 2017). This requires a significant investment by underwriters in understanding the level of protection provided through the wide variety of protection technologies available (which is particularly important since some have suggested that one third of all cyber vulnerabilities result from the use of security software (Harrington, 2017)). Meanwhile, ever-evolving (and increasingly sophisticated) attack methods may make some protection technologies quickly obsolete while some attacks are so sophisticated that it does not matter how much a company has invested in cyber security (Marsh & McLennan Companies, 2016). Further, a comprehensive picture of the level of resilience against cyber risk also requires an assessment of risk management, business continuity planning and information technology policies and processes. Many incidents occur as a result of human error or even a failure to respond to warnings provided by protection technologies - not a technical failure in the protective technology itself (Marsh & McLennan Companies, 2016).

A number of the insurance sector respondents to the OECD questionnaire indicated that they are examining the value of different protection technologies and security practices with the aim of improving their ability to assess risk at different companies, sometimes in partnership with cyber security service providers. Management consulting firms (e.g. McKinsey) and cyber security companies are also providing cyber security assessments services, and in some cases (e.g. Symantec), are offering standardised application forms to support cyber insurance underwriting. There are some models that specifically assess the level of risk at a company with a given set of protective technologies, security procedures and policies (e.g. Cyence) - with some reported success in terms of differentiating risk across different security postures (Marsh & McLennan Companies, 2016; Insurance Journal, 2017).

As the importance of cyber risk has increased, a number of private sector companies have started to develop cyber security ratings that can be used by underwriters (e.g. BitSight ratings, FICO Enterprise Security Scores, Security Effectiveness Scores (PGP Corporation and Ponemon Institute), etc.) based on assessments of cyber security practices as well as observable data on cyber attacks. Providers of these ratings have
claimed some success in identifying a correlation between their ratings and cyber-related losses, although there may be some risk in overreliance on these ratings (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2017). As a result of the increasing use of these types of security ratings, a number of US companies (including many of the security rating organisations) released a set of shared principles for the development and reporting of security ratings, leveraging some good practices that have been put in place by credit rating agencies (U.S. Chamber of Commerce, 2017).

Governments can play a role in facilitating the assessment of risk management technologies and processes by promoting the establishment and adoption of cyber security standards and methodologies for assessing compliance against these standards (or by encouraging adoption of existing international standards such as ISO/IEC 27001). Examples of such standards include the US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity and the UK Cyber Essentials. Companies often perceive government information and advice as more impartial (relative to cyber security vendors interested in selling protection technologies) and some have suggested a government role in certifying the effectiveness of specific protection technologies. In some countries, government certification schemes do exist for some cyber security related services. For example, in the United Kingdom, the public National Technical Authority for Information Assurance (CESG) provides certification of cyber security consultancies and incident response companies (Department for Media, Culture & Sports, 2016). In the United States, the Department of Homeland Security is offering to undertake cyber security assessments and technology reviews for certain companies (a service advertised as a policyholder benefit by at least one insurance company) (Carrier Management, 2016). In Europe, the European Commission recently announced the establishment of a European cybersecurity certification framework for products and services that are important for the functioning of the Digital Single Market (European Commission, 2017).

Sectoral regulators could also contribute to the assessment of cyber risk management practices by establishing guidance for the companies they regulate on their expectations for cyber resilience (which may provide some assurance to underwriters about the level of cyber resilience in regulated companies). Financial sector regulators normally include cyber risk within the scope of their supervisory activities and a number have established specific guidance on cyber security practices for regulated entities. For example, the Office of the Superintendent of Financial Institutions Canada (2013) has published "Cyber Security Self-Assessment Guidance" which sets out desirable cyber security practices. The G7 Finance Ministers and Central Bank Governors have established the “G7 Fundamental Elements of Cyber Security for the Financial Sector” which provides a framework to ensure financial institutions are properly managing cyber risks. Governments might even consider minimum cyber security standards which all companies must achieve (Eling and Wirfs, 2016).

So far, there is no convergence across the insurance sector in terms of an approach to rating the effectiveness of different technologies or processes/policies. As outlined in Table 5.1, four of the five main data aggregation/harmonisation initiatives collect some information on company attributes and practices although there is little harmonisation, except at the level of basic company data (employees, revenue, sector, etc.). The two data schemes involving the catastrophe modelling sector include similar "company risk attributes" (such as number and type of confidential records and measures of business interruption potential) although apply very different approaches to collecting information on company risk management practices (the Cambridge Centre Risk Studies uses a single
user-generated rating of cyber security practices rather than a set of criteria related to the use of different risk management practices. The AIR Worldwide and US Cyber Incident and Data Analysis Working Group include data on some similar risk management practices (although more detail is sought under the AIR Worldwide framework).

Table 5.1. **Data collected (or planned for collection) by different data aggregation/harmonisation initiatives**

<table>
<thead>
<tr>
<th>Basic company data</th>
<th>US Cyber Incident Data and Analysis Working Group</th>
<th>Advisen CRO Forum</th>
<th>AIR Worldwide Cyber Exposure Data Standard</th>
<th>Cambridge Centre for Risk Studies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sector (list)</td>
<td>Sector2</td>
<td>Sector2</td>
<td>Sector2</td>
<td></td>
</tr>
<tr>
<td>Number of employees2</td>
<td>Number of employees2</td>
<td>Number of employees2</td>
<td>Number of employees2</td>
<td></td>
</tr>
<tr>
<td>Annual revenue2</td>
<td>Annual revenue2</td>
<td>Annual revenue2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location and geographical footprint</td>
<td>Location and geographical footprint</td>
<td>Location and geographical footprint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company risk attributes</td>
<td>Registered domain names</td>
<td>IP addresses</td>
<td>Cloud service providers2</td>
<td></td>
</tr>
<tr>
<td>Internet-based revenue</td>
<td>Internet-based revenue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revenue dependent on cloud services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number and types of confidential records2</td>
<td>Number and types of confidential records (PII, PCI, PHI)2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business interruption cost</td>
<td>Business interruption from internet failure2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business interruption from cloud service failure</td>
<td>Business interruption and financial losses from payment system service failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach history (5-year)</td>
<td>Cyber security score (user generated)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management practices</td>
<td>Officer responsible for cyberinformation security</td>
<td>Chief Information Security Officer, Chief Privacy Officer, Chief Digital Officer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management framework, best practice or standard used, standard certification</td>
<td>Standards: (ISO 27001, NIST 800-53, Cyber Essentials, PCI data security standards, etc),</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of time that resources have been dedicated to cyber security</td>
<td>Qualitative score – IT maturity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are risk management practices formalised as a policy</td>
<td>Qualitative score – IT maturity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is cyber security integrated into enterprise risk management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are policies and procedures risk-informed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

5. ADDRESSING CHALLENGES TO CYBER INSURABILITY

ENHANCING THE ROLE OF INSURANCE IN CYBER RISK MANAGEMENT © OECD 2017
<table>
<thead>
<tr>
<th>Incident type</th>
<th>US Cyber Incident Data and Analysis Working Group</th>
<th>Advisen</th>
<th>CRO Forum</th>
<th>AIR Worldwide Cyber Exposure Data Standard</th>
<th>Cambridge Centre for Risk Studies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data theft (PII, financial data, health records, other)</td>
<td>Privacy – unauthorised contact or disclosure</td>
<td>Third party data confidentiality breach</td>
<td>Cyber security data and privacy breach (Lloyd's CY)²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data theft - intellectual property</td>
<td>Data (unintentional disclosure, physically lost or stolen, malicious breach)</td>
<td>First party data confidentiality breach</td>
<td>Cyber security property damage (Lloyd's code CZ)² or Cyber security data and privacy breach (Lloyd's CY)²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Industrial espionage</td>
<td>System failure</td>
<td>--</td>
<td>Own system malfunction</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>SCADA or Industrial Control System</td>
<td>Industrial controls &amp; operations</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Configuration error</td>
<td>IT – configuration/implementation errors</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Web page defacement</td>
<td>Outage</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Outage</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Malware</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Zero-Day malware attack</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Destructive WORM</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Distributed Denial of Service</td>
<td>Network/website disruption</td>
<td>Network communication malfunction</td>
<td>Cyber security data and privacy breach (Lloyd's CY)²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--</td>
<td>--</td>
<td>Inadvertent disruption of third party system</td>
<td>--</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third-party event</td>
<td>--</td>
<td>Disruption of external digital infrastructure</td>
<td>--</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage/back-up failure</td>
<td>IT – processing errors</td>
<td>Deletion or corruption of own or third party data</td>
<td>--</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--</td>
<td>--</td>
<td>Cyber extortion</td>
<td>Encryption of own or</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

1. ENHANCING THE ROLE OF INSURANCE IN CYBER RISK MANAGEMENT © OECD 2017
2. Lloyd's CY: Cyber security and privacy breach
3. Lloyd's CZ: Cyber security property damage
## 5. Addressing Challenges to Cyber Insurability

<table>
<thead>
<tr>
<th>US Cyber Incident Data and Analysis Working Group</th>
<th>Advisen</th>
<th>CRO Forum</th>
<th>AIR Worldwide Cyber Exposure Data Standard</th>
<th>Cambridge Centre for Risk Studies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware/extortion</td>
<td>--</td>
<td>--</td>
<td>Misuse of system for defamatory systems</td>
<td>--</td>
</tr>
<tr>
<td>Phishing</td>
<td>Phishing, spoofing, social engineering</td>
<td>Cyber fraud/cyber theft</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Natural or man-made (physical) peril</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Cyber terrorism</td>
</tr>
<tr>
<td>Physical sabotage</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Categories for incident causes (network intrusion, insider attack, lost device accident/human error) that cover multiple categories</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Non-financial indicators of impact (severity, affected assets, type of impact, outcome of incident, duration of interruption/outage, security response to incident, number of records compromised and level of sensitivity)</td>
<td>Non-financial indicators of impact (affected count, source of loss, type of loss)</td>
<td>Breach of privacy [compensation]</td>
<td>Security breach expense limit</td>
<td>Breach of privacy event</td>
</tr>
<tr>
<td>Credit monitoring</td>
<td>Breach of privacy</td>
<td>Security breach</td>
<td>--</td>
<td>Breach of privacy event</td>
</tr>
<tr>
<td>Legal costs</td>
<td>Regulatory and defence (excluding fines and penalties)</td>
<td>Fines limit</td>
<td>Regulatory and defence</td>
<td></td>
</tr>
<tr>
<td>PCI fines and assessments</td>
<td>Fines and penalties</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Investigation/forensics</td>
<td>Incident response costs</td>
<td>--</td>
<td>Incident response costs</td>
<td></td>
</tr>
<tr>
<td>Victim notification</td>
<td>Reputational damage (excluding legal protection)</td>
<td>Public relations limit</td>
<td>Reputational damage</td>
<td></td>
</tr>
<tr>
<td>Public relations/reputation</td>
<td>Cyber ransom and extortion</td>
<td>Extortion limit</td>
<td>Financial theft and/or fraud</td>
<td></td>
</tr>
<tr>
<td>Theft</td>
<td>Financial theft and/or fraud</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Liability</td>
<td>Communication and media [liability]</td>
<td>Media liability limit</td>
<td>Multi-media liabilities (defamation and disparagement)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Directors and officers</td>
<td>--</td>
<td>Liability - directors and</td>
<td></td>
</tr>
</tbody>
</table>

122

ENHANCING THE ROLE OF INSURANCE IN CYBER RISK MANAGEMENT © OECD 2017
Data for managing accumulation risk

A third critical element in quantifying cyber risk exposure is assessing the potential for correlation (accumulation) risk. In the case of natural catastrophe or terrorism modelling, this can mostly be accomplished by understanding the geographical location of buildings and infrastructure exposed to damage as most natural catastrophes and terrorism attacks will only affect a limited geographical area.9 Cyber risk, on the other hand, could be correlated on a global basis given the dependence of companies around the world on common technologies and service providers.

As noted above, modelling firms and other insurance sector organisations are developing a broad range of scenarios to help insurance companies understand their exposure to incidents that could lead to correlated losses. For example, RMS has recently released new data exfiltration, financial theft, cyber extortion, denial of service attack and cloud service provider failure scenarios involving widespread impacts across a broad range of companies (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2017). RMS has also developed several scenarios related to physical damage (e.g. cyber induced fires in commercial office buildings or industrial plants, explosions on

---

1. The Cambridge Centre for Risk Studies includes notification costs as part of the breach of privacy event loss type (the CRO Forum includes notification costs as incident response costs).
2. Included in Lloyd's (2016c) Cyber Core Data Requirements (also agreed by AIR Worldwide and RMS)

oil rigs, cargo theft and regional power outages) (Carrier Management, 2017). AIR Worldwide's modelling software provides capacities to model data theft, vulnerable or unsupported software, denial-of-service attacks, cloud service provider failure, payment processor failure, domain name server provider failure, cyber extortion, blackouts, internet service provider failure and a compromise of public key infrastructure (e.g. encryption keys, certificate authentication, etc.) (AIR Worldwide, 2016b). JLT Re has developed a number of scenarios based on various types of information technology outages (JLT Re, 2017). As noted above, Lloyd's has committed to developing 8-10 accumulation scenarios to help its syndicates manage accumulation risk (Lloyd's, 2016a).

Equally important is the collection of data to allow for the mapping of potential accumulation risk. Several respondents to the OECD questionnaire indicated that they are collecting such information through the underwriting process (e.g. the type of software that is being used). As outlined in Table 5.1, the AIR Worldwide and Cambridge Centre for Risk Studies data schemes recommend collection of various data points that could support the assessment of accumulation risk, including data related to the identification of cloud service providers, IP addresses and registered domain names, as well as various indicators of the business interruption impact of a failure of a company's internet service provider, cloud service provider or payment system service provider.

**Addressing the challenges to understanding cyber insurance coverage**

As noted in Chapter 4, misunderstanding about the need for - and utility of - cyber insurance coverage is likely to be an important impediment to demand for such coverage. The misunderstanding results from both the difficulty in determining where there may be gaps in terms of the coverage provided by traditional policies, as well as the complexity (and wide diversity) of stand-alone cyber insurance coverage terms and conditions. There are a number of potential approaches to addressing these issues (and a few examples of efforts to do so) ranging from building awareness about coverage offered in the market to market and regulatory initiatives aimed at promoting (and/or ensuring) harmonisation/standardisation of coverage terms and conditions.

Insurance brokers play a critical role in helping companies identify the coverage needed and the form of coverage best suited to their needs. The brokers and broker associations that responded to the OECD questionnaire identified various methods to raise awareness of cyber risks and coverage options among their clients, including conferences and seminars, publications and customer surveys. One brokerage specifically mandates all of its brokers to discuss cyber coverage upon renewal of their policies and offer an indication of the premium they may expect. This is consistent with other surveys that found that the vast majority of brokers (close to 90%) play an active role in educating their clients about cyber risks (Council of Insurance Agents and Brokers, 2016). Similarly, comments from insurance underwriters highlighted the role of brokers in educating clients and their efforts to ensure that brokers had sufficient knowledge of the cyber insurance products available in the market. Many insurance associations have also developed educational materials for business on protecting against cyber risks and available insurance options, including in France ("Anticiper et minimiser l'impact d'un cyber risque sur votre entreprise: TPE, PME, vous êtes concernées!"), the United Kingdom ("Making Sense of Cyber Insurance: A Guide for SMEs"), Canada ("Cyber Liability" website) and the United States ("Cybersecurity and identity theft coverage: The state of the industry") (Fédération française de l'assurance, 2017; Association of British Insurers, 2016; Insurance Bureau of Canada, n.d.; Insurance Information Institute, n.d.).
In some countries, different stakeholders have come together to provide greater clarity on the insurance coverage of cyber risk. In France, for example, representatives of the business community, brokers, insurance companies, reinsurance companies, legal firms and government collaborated on a research project aimed at providing clarity on types of cyber risks, where these risks are covered by different insurance policies and any gaps that might exist (see Box 5.3).

**Box 5.3. Building awareness on the insurance coverage for cyber risk: France**

In France, a research group involving business, reinsurance companies, researchers and government agencies was established by a public research institute (IRT System X) to examine how companies can better measure and manage their exposure to cyber risk, including through risk transfer to reinsurance markets. One outcome of the project was the development of a matrix outlining the types of potential losses that companies could face as a result of cyber incidents and the types of insurance policies that would normally provide coverage for those losses based on practices in the French insurance market (a simplified version of that matrix is provided in Figure 5.1). The research led to the identification of important gaps in coverage in the market in areas such as reputational losses, ransoms, and fines and penalties (similar to other markets). It also to the establishment of a larger working group that aims to make specific recommendations on how to improve cyber resilience and risk coverage.

**Figure 5.1. Insurance coverage for cyber risks in France**

<table>
<thead>
<tr>
<th>Event</th>
<th>Indirect cyber attacks</th>
<th>Targeted cyber attacks</th>
<th>Human error</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage</td>
<td>Property</td>
<td>Property</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Transport</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>N/A</td>
</tr>
<tr>
<td>Loss</td>
<td>N/A</td>
<td>N/A</td>
<td>Fraud</td>
<td>N/A</td>
</tr>
<tr>
<td>Operating losses</td>
<td>Property</td>
<td>Property</td>
<td>N/A</td>
<td>Cyber</td>
</tr>
<tr>
<td>IT costs</td>
<td>Property</td>
<td>Property</td>
<td>N/A</td>
<td>Cyber</td>
</tr>
<tr>
<td>Costs due to violation of personal data</td>
<td>N/A</td>
<td>N/A</td>
<td>Cyber</td>
<td>N/A</td>
</tr>
<tr>
<td>Costs of re-establishing e-reputation &amp; communication</td>
<td>Property</td>
<td>Property</td>
<td>Cyber</td>
<td>Cyber</td>
</tr>
<tr>
<td>Legal protection</td>
<td>N/A</td>
<td>N/A</td>
<td>Cyber</td>
<td>Cyber</td>
</tr>
<tr>
<td>Cost of liability for loss or injury caused to third parties</td>
<td>Property</td>
<td>Property</td>
<td>Liability</td>
<td>Liability</td>
</tr>
<tr>
<td>Fines and penalties</td>
<td>Property</td>
<td>Property</td>
<td>Liability</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*Source: Adapted from IRT SystemX (2016).*
A number of insurance sector respondents to the OECD questionnaire identified the need for further harmonisation (or standardisation) of cyber insurance coverage. The Geneva Association (2016), a research institution funded by large insurance companies, has also indicated that it might be "important to establish standards with regard to definitions, coverages and pre-coverage risk assessment" as a means to address challenges to the development of the cyber insurance market (particularly as new companies enter the market). Some have also suggested that more harmonisation in terms and conditions could facilitate market entry (and therefore capacity and competition) as new entrants could build policies based on standard language and reduce the potential for claims disputes (Deloitte, 2017). However, other respondents highlighted the risks of any regulatory intervention aimed at achieving standard terms and conditions for cyber insurance, noting that such an intervention could impede innovation and choice in the market and also risks becoming quickly irrelevant (or in need of update) as a result of the fast-evolving nature of cyber risk.

As noted in Chapter 3, there are some indications that market development has led to increased harmonisation across policies (although significant variation is still the norm). There have been suggestions that an increasingly competitive market will continue this trend towards uniform terms and conditions (The Geneva Association, 2016). Some market practices, including product development/packaging by brokers, reinsurance companies, the Insurance Services Office and even modelling firms, could encourage greater harmonisation. Automation of product sales through websites could also play a role in increasing harmonisation (at least one company has launched a comparison engine for cyber policies in the United States (Sclafane, 2016)). Some insurance associations are also supporting greater harmonisation of policy language. For example, the German Insurance Association (GDV) has released a set of non-binding model conditions for use by insurance companies offering cyber insurance coverage to SMEs (Gesamtverband der Deutschen Versicherungswirtschaft, 2017). A similar effort is also underway in Austria (Insurance Europe, n.d.).

Another potential means of reducing uncertainty would be to mandate that cyber risks be covered in traditional policies (i.e. eliminate the need for stand-alone cyber insurance products and therefore any confusion on where cyber risks would be covered). As noted in Chapter 3, some insurance companies are moving in this direction by explicitly providing coverage for cyber risks in traditional policies. Companies might prefer this approach as many would consider cyber risk to be a peril like any other peril normally covered in traditional policies. However, there are a number of advantages to covering cyber risks under a stand-alone policy including the specific expertise that is being developed in understanding and quantifying cyber risks, helping companies protect against those risks and supporting their response to cyber incidents (which might not occur if cyber risk were treated as a peril in multi-peril policies). Despite the complexity noted above, stand-alone policies might also provide greater clarity on coverage of cyber risks than the general language included in traditional policies (JLT Re, 2017). There are precedents in terms of other emerging risks that were carved out of traditional policies into stand-alone specialty lines as claims experience (and loss potential) grew, such as in the case of directors and officers liability policies (Fitch Ratings, 2017).

Another approach would be to seek greater transparency at the level of individual policies on the exact scope of coverage for cyber risks. The UK Prudential Regulation Authority (2017) published a supervisory statement in July 2017 setting out its expectations for the management of cyber insurance underwriting risk which should encourage (re)insurance companies to provide greater clarity on the coverage that they
are providing for cyber risks in traditional policies (and also encourage more robust management of "non-affirmative" or "silent" coverage) (see Box 5.4).

Box 5.4. Prudential Regulation Authority supervisory statement on cyber insurance underwriting risk

In July 2017, the Bank of England Prudential Regulation Authority (PRA) issued a supervisory statement outlining its expectations with respect to the management of cyber insurance underwriting risk. The statement applies to all UK non-life insurance and reinsurance groups (including the Society of Lloyd's and managing agents) and includes cyber insurance underwriting risk related to both affirmative (explicit) and non-affirmative (implicit or "silent") coverage of cyber risks.

The supervisory statement sets out the PRA’s expectation that companies are able to identify, quantify and manage both types of cyber exposure and will have clear Board-level strategies and risk appetite statements for these risks (such as strategies for managing non-affirmative cyber risk, rules related to the overall amount of coverage provided and/or limits for specific industries). It sets out that, at a minimum, companies should be able to provide management with clear articulations of their risk appetite, exposure metrics for both affirmative and non-affirmative exposure and stress testing approaches for potential loss aggregation at a return period of up to 1 in 200 years).

It also sets out specific expectations for the management of non-affirmative cyber risk (defined as "insurance policies that do not explicitly include or exclude coverage for cyber risk") aimed at reducing unintended exposure to cyber risk, suggesting that companies should: (i) offer explicit cover and adjust the premium accordingly; (ii) introduce robust wording exclusions; or (iii) attach specific limits to the coverage provided. Companies are able to offer coverage for cyber risk in traditional lines of business without a corresponding premium increase although the PRA would expect a comprehensive assessment of the implications of offering such coverage and suggests that the coverage be made explicit in policy wordings.

Source: Prudential Regulation Authority (2017)

Other approaches to supporting greater market capacity

While improving capacity to quantify cyber risks and addressing the challenges to understanding cyber coverage are likely to be the most important means to improving insurance market capacity, other approaches have also been suggested. These include various types of tax incentives to: (i) encourage insurance purchase; (ii) support the accumulation of reserves by insurers to cover peak risks; or (iii) support transfer of cyber risks to capital markets (Swiss Re, 2017; Eling and Wirfs, 2016). In the United States, a Data Breach Insurance Act (H.R. 6032) has been introduced in Congress to provide tax credits equal to 15% of the cost of cyber insurance premiums (subject to the adoption of the NIST Framework for Improving Critical Infrastructure Cybersecurity) (Council of Insurance Agents and Brokers, 2016). Some have also suggested that mandatory purchase requirements may be necessary for cyber risks, particularly for liability risks (Swiss Re, 2017) which, if effectively enforced, would ensure a sufficient pool of insureds (and thereby support insurability).

Several analyses have noted the potential benefits of an insurance pool for addressing market capacity issues (Swiss Re, 2017; Eling and Wirfs, 2016; Carbone and Ryan, 2016), such as:

- **Increased market capacity:** Pooling of risks creates diversification benefits that would allow the pool to carry a higher level of risk than the sum of risk that can
be covered by its members individually (Eling and Wirfs, 2016). A pooling mechanism might also facilitate the entry of smaller firms that wish to gain experience in the market while limiting their liability (Swiss Re, 2017). The diversification benefits and reduced uncertainty inherent in a large pool might also lead to lower prices for coverage (Eling and Wirfs, 2016).

- **Harmonisation of coverage:** Pooling mechanisms would normally only pool the risks from similar (if not identical) coverage offerings, as the sharing of risk would otherwise be too complicated. As a result, a pooling mechanism would normally lead to greater standardisation of products (Carbone and Ryan, 2016; Eling and Wirfs, 2016).

- **Sharing of information about threats and incidents:** A pool would have access to the claims experience of its members and therefore could make a contribution to reducing the gap in data availability for underwriting and modelling cyber risk. Pool members could also share information on threats and vulnerabilities (Carbone and Ryan, 2016) and potentially the effectiveness of different security practices. A pooling mechanism that covers a large share (or all) of the market should also reduce the incentive for companies to gain market share by reducing underwriting standards (and thereby increase the contribution of insurance to the overall level of cyber security) (Carbone and Ryan, 2016).

- **Facilitating the transfer of cyber risk to reinsurance and capital markets:** By establishing a pool of similar risks, a pooling mechanism can make it easier (and less expensive) to transfer risk to international reinsurance and capital markets (see Box 5.5) (Carbone and Ryan, 2016). If deemed necessary, a pooling mechanism could also establish a structure for providing a government back-stop for cyber risk (a number of analyses have suggested that a government backstop may be necessary to: (i) cover the most extreme events which may be otherwise uninsurable (Swiss Re, 2017); (ii) cover cyber terrorism and cyber warfare (JLT Re, 2017); or (iii) as a means of reducing the overall level of uncertainty in the market (BNY Mellon, 2016)).

Pooling mechanisms have been created in a number of countries to address market capacity for covering various perils, including aviation, nuclear, terrorism, earthquake, wind and flood (or a range of natural perils). Pools have also been established for particular business lines such as accident and health in the United States in the 1970s (Carbone and Ryan, 2016), environmental liability in Italy and directors and officers liability coverage in Germany (Eling and Wirfs, 2016). Some pools have been established on a temporary (or renewable) basis and have been abolished as the market developed (e.g. the US accident and health reinsurance pools (Carbone and Ryan, 2016)). However, most have become quasi-permanent organisations leading many to suggest that an exit strategy would be difficult to implement. Pools can also limit market competition and innovation (Carbone and Ryan, 2016) and many pools operate with premiums that are not differentiated by level of risk.

Given the significance of liability in cyber losses, another approach to increasing market capacity might be to restrict (or otherwise reduce) the potential liability that companies might face as a result of a cyber incident (and therefore reduce the potential maximum losses that insurers could face). In the United States, for example, the *SAFETY Act* adopted after the September 11th terrorist attacks limited the legal damages that firms
providing anti-terrorism technologies could face (where those technologies had been approved by the Department of Homeland Security) (Swiss Re, 2017). Changes to the framework for establishing liability could also reduce the potential liability that companies face, for example, by limiting the amount of compensation that can be provided where no damages have been identified, requiring that defendant's legal fees are paid by plaintiffs when lawsuits are not successful or limiting the role of litigation funding - although these kinds of interventions may have other unintended consequences.

Box 5.5. Insurance-linked securities covering cyber risk: challenges

Insurance-linked securities (ILS), such as catastrophe bonds, sidecars, industry-loss warranties and other instruments, were developed in the 1990s and have played an increasing role in providing coverage for peak losses (given the much larger potential for capital markets to absorb losses) (an assessment of their use in the context of other catastrophe perils is provided in OECD (2011)). ILS have mostly been issued to cover property catastrophe risks although products have also been issued for other business lines, including life, accident and health, casualty lines and even operational risks in one recent case (Swiss Re, 2017). The development of the ILS market has benefitted from increasing confidence in the models and industry loss estimates that underpin many ILS issuances as well as from the availability of high-quality meteorological, hydrological and geological data that can also be used as a trigger for payouts.

The potential for issuing ILS to cover cyber losses faces a number of challenges, not least the lack of available data and modelling (let alone confidence in that modelling) (Swiss Re, 2017; Amaral, 2016) and the lack of standard definitions (Morris, 2017). Long-tail, unpredictable liability risks, which are often the most substantial part of cyber losses, tend to be less attractive to capital markets investors (Amaral, 2016). There is also a higher potential for the triggering event to have an impact on bond and equity markets, reducing the diversification benefits that have attracted investors to ILS covering property catastrophe risks. There have also been few options for a viable parametric or index-based trigger, which normally must be easily understandable and observable (from the investors' perspective) while sufficiently correlated with actual losses (from the issuers' perspective). Recently, however, PCS, a provider of industry loss estimates for other perils that are often used in the ILS market, has announced its intention to develop industry loss estimates for significant cyber incidents ("PCS Global Cyber") that will seek to aggregate claims data from the insurance industry for incidents with potential industry-wide losses above USD 20 million (Verisk, 2017). The data confidentiality breach at Equifax has reportedly been designated by PCS as the first such event for which an industry loss estimate will be calculated (Artemis, 2017).

A pooling mechanism could potentially facilitate the structuring of an ILS issuance for cyber risk by providing the possibility of triggering the ILS on an industry-loss basis or even on a proportional basis based on losses suffered by the pool. The one successful issuance of an ILS linked to operational risks (Credit Suisse's "operational risk bond") involved the issuance of an insurance policy for operational risks (which defines the terms and conditions of coverage) with the operational risk bond providing a layer of coverage above the insurance policy, triggered when annual aggregate losses covered by the insurance policy exceed a certain threshold (Artemis, 2016).

1. An ILS transaction involving both cyber and terrorism risk was reported in September 2017 although the specific details of that transaction have not been publicly disclosed (Insurance Day, 2017).

Finally, insurance regulators and credit rating agencies can have an important impact on the amount of coverage the market is willing to provide. The level of uncertainty related to cyber risks - and the dearth of available data and models - have led some insurance regulators and rating agencies to take a cautious approach in their oversight of cyber risk underwriting (Carbone and Ryan, 2016). Fitch Ratings (2017), for example, has taken the view that a downward trend in pricing for cyber insurance would be a ratings concern due to the more limited availability of actuarial data relative to mature lines of business. While this caution is reasonable given the level of uncertainty, an abundance of caution could reduce the willingness of insurance companies to underwrite cyber risk.
5. ADDRESSING CHALLENGES TO CYBER INSURABILITY

Notes

1. For example, Marsh Cyber IDEAL is a predictive frequency and severity model for data confidentiality breaches based on past incidents (e.g. an estimate of return period for suffering from a given loss based on number and types of records held) (Marsh & McLennan Companies, 2016). Cyence has developed an economic modelling platform for predicting the frequency and severity of cyber incidents based on various company characteristics, which is reportedly being used for both underwriting and accumulation management (Marsh & McLennan Companies, 2016). JLT has developed a model for companies to measure their exposure based on various company characteristics, such as sector, number of records and security practices for data breach, loss of data, network interruption and cyber extortion incidents which, while targeted at companies (policyholders), may also be useful for insurers (JLT Re, 2017). There is also some academic work on calculating incident rates by sector (Romanosky, 2016). Commercial modelling firms are also working on the developing probabilistic models, particularly for the incident types for which there is better data (Hancock, 2017c).

2. Defined as “coverage in respect of first or third party costs, expenses or damages due to a breach (or threatened breach) of cyber security and/or privacy of data, that does not include damage to physical property.”

3. Defined as “coverage in respect of first or third party costs, expenses or damages due to a breach of cyber security that includes damage to physical property.”


5. ISO and Perils collect data from insurance companies upon the occurrence of a natural catastrophe that meets a certain threshold, anonymises the data and then publishes industry-wide loss estimates. These estimates are often used as a trigger for capital market risk transfer instruments.

6. The AIR Worldwide (2016a) cyber exposure data standard does not include a specific categorisation related to incident type although AIR Worldwide, RMS and Lloyd's have agreed to use common peril codes in their data standards. The incident categorisation in Cambridge Centre for Risk Studies (2016), which was developed with RMS and Lloyd's, includes the common peril codes.

7. For example, the US Cyber Incident Data and Analysis Working Group includes nearly 20 incident types (and sub-types) relative to approximately 11 used by the CRO Forum and 3 used by the Cambridge Centre for Risk Studies. In addition, some incident types (e.g. physical peril, unauthorised data collection) are only included in one of the five data aggregation initiatives.

8. The Cyber Core Data Requirements developed by AIR Worldwide, RMS and Lloyd's includes a few common data points related to company attributes, including sector, number of employees, annual revenue, number and types of confidential records, internet business interruption potential and identification of cloud service providers. These are reflected to some extent (although not completely) in the current AIR Worldwide and Cambridge Centre for Risk Studies data schemes.
9. For the purposes of managing contingent business interruption exposures, some models are beginning to assess risks related to disruptions in global supply chains which could have implications far beyond a particular geographic region.

10. Chapter 4 also discussed challenges in terms of cyber risk awareness and particularly the need for companies to invest in quantifying their exposure to cyber risk. There are several examples of ways to address these challenges, from awareness campaigns to the efforts of brokers to help companies quantify their exposures, including through the use of models (which also related to the data challenges outlined in the previous section). A comprehensive discussion of these issues was deemed to be outside the scope of this report.

11. The opposite is also possible - i.e. mandate that all cyber risks be excluded from traditional policies.

References


5. ADDRESSING CHALLENGES TO CYBER INSURABILITY


5. ADDRESSING CHALLENGES TO CYBER INSURABILITY


JLT Re (2017), Unlocking the potential of the cyber market: JLT Re Viewpoint, JLT Re, London.

Lloyd’s (2016a), Lloyd’s Cyber-Attack Strategy, Lloyd's, London.

Lloyd’s (2016b), Realistic Disaster Scenarios: Scenario Specification (January 2016), Lloyd's, London.


Lloyd’s (2015), Lloyd's Risk Codes: Guidance and Mappings (April), Lloyd's, London.


OECD (forthcoming), Review of surveys on digital security risk management practices in businesses.


Swiss Re (2016), Cyber: in search of resilience in an interconnected world, Swiss Re, Zurich.


