Cyber Risk Underwriting

Identified Challenges and Supervisory Considerations for Sustainable Market Development

December 2020

About the IAIS

The International Association of Insurance Supervisors (IAIS) is a voluntary membership organisation of insurance supervisors and regulators from more than 200 jurisdictions. The mission of the IAIS is to promote effective and globally consistent supervision of the insurance industry in order to develop and maintain fair, safe and stable insurance markets for the benefit and protection of policyholders and to contribute to global financial stability.

Established in 1994, the IAIS is the international standard setting body responsible for developing principles, standards and other supporting material for the supervision of the insurance sector and assisting in their implementation. The IAIS also provides a forum for Members to share their experiences and understanding of insurance supervision and insurance markets.

The IAIS coordinates its work with other international financial policymakers and associations of supervisors or regulators, and assists in shaping financial systems globally. In particular, the IAIS is a member of the Financial Stability Board (FSB), member of the Standards Advisory Council of the International Accounting Standards Board (IASB), and partner in the Access to Insurance Initiative (A2ii). In recognition of its collective expertise, the IAIS also is routinely called upon by the G20 leaders and other international standard setting bodies for input on insurance issues as well as on issues related to the regulation and supervision of the global financial sector.

International Association of Insurance Supervisors
c/o Bank for International Settlements
CH-4002 Basel
Switzerland
Tel: +41 61 280 8090 Fax: +41 61 280 9151
www.iaisweb.org

This document was prepared by the Cyber Underwriting Small Group in consultation with IAIS Members.

This document is available on the IAIS website (www.iaisweb.org).

Contents

Executive summary 4
Introduction 7
Sources of information and approach to analysis 7
1 Cyber insurance market 9
1.1 Products and services 9
1.2 Size of market 12
1.2.1 Cyber insurance as a fraction of the overall insurance market 14
1.2.2 Cyber insurance take-up rates and limits 14
1.2.3 Cyber insurance vs cyber losses 15
1.2.4 Pricing and underwriting performance 15
1.3 Cyber reinsurance 16
2 Key findings from literature review and stakeholder engagement 17
2.1 Measurement of risk exposure 17
2.1.1 Evolving nature of cyber risk 18
2.1.2 Limited loss experience 18
2.1.3 Difficulties in assessing policyholder vulnerabilities 21
2.1.4 Accumulation risk 23
2.1.5 Non-affirmative exposure 24
2.2 Clarity of policies 26
2.2.1 Overlapping coverage 26
2.2.2 Non-Affirmative coverage 26
2.2.3 Treatment of ransoms, fines, terrorism and war risk 27
3 Regulatory and Supervisory developments 28
3.1 Overview of responses and main findings 29
3.1.1 Monitoring cyber risk underwriting 30
3.1.2 Supervisory framework on cyber risk underwriting 31
3.1.3 Supervisory capacity for monitoring cyber risk underwriting 32
3.1.4 Supervisory concern on cyber risk underwriting 32
4 References 33

Executive summary

Cyber insurance presently constitutes a relatively small but growing portion of the overall non-life insurance market. As digitisation, interconnectedness and cyber threats continue to expand, cyber insurance has the potential to become an increasingly more significant part of the non-life market and to play a greater role in mitigating the risks associated with cyber incidents.

In view of the potential scale and pace of the growth of the cyber insurance market and the ubiquitous and significant nature of cyber risk, cyber insurance underwriting has increasingly attracted supervisory attention.

For these reasons, the IAIS included cyber risk underwriting among the issues presenting opportunities, challenges and risks related to its mission, with a view to assessing and responding to them in the context of its 2020-2024 Strategic Plan (under High Level Goal 1).

As a preparatory step towards developing a strategic approach to how supervisory practices can foster sustainable cyber risk underwriting, in the second half of 2019 the IAIS appointed a Cyber Underwriting Small Group (CUSG) of experts from its Member supervisors and the OECD to:

- Carry out a stock-take of relevant literature on development of the cyber underwriting market and – in particular – the risks and opportunities for microprudential soundness, fair conduct of business and broader financial sector stability;
- Carry out a stock-take of supervisory practices in different jurisdictions aimed at promoting sustainable cyber insurance underwriting;
- Consider possible implications of the above for the future work of the IAIS; and
- Prepare a report with findings and recommendations for a strategic approach as well as possible follow-up work for consideration by the IAIS Executive Committee.

The results of this work were reported to the Executive Committee, which acknowledged the findings and supported the proposed further work in line with the findings of the report.

The findings indicate that current cyber underwriting practices, while serviceable, are not yet optimal, particularly due to issues surrounding the measurement of risk exposures. Generally, insurers manage their exposure to policyholders' cyber risk by seeking to employ prudent policy limits, thereby containing the exposure to single risk sources and mitigating the risk measurement challenges. However, the nature of cyber risk and the complexity of supply-chains may lead to loss accumulation and it is not clear that current practices permit adequate assessment and limitation of this concern – particularly as regards so-called "non-affirmative cyber coverage".[1] Although insurers are aware of this issue, and some supervisors and insurers are taking important steps to limit the risk, at this time non-affirmative cyber coverage may still present a dangerous hidden amplifying factor of insurers' risk exposures, as it can affect other type of policies (eg Property and Casualty) that have much higher limits.

On the supervisory front, the findings indicate that supervisory intensity (eg frequency of assessment) and specific toolbox development (eg use of stress-tests) are generally proportionate to the relative importance of the cyber underwriting market, which is generally limited at this time. There is supervisory awareness of the challenges posed by this line of

[1] See par. 2.1.5 for a definition of non-affirmative cyber coverage.

business, and growing attention, as shown by ad-hoc data collection initiatives launched by the majority of the IAIS Members surveyed, to these risks.

However, with few exceptions, supervisors have not yet issued specific guidance to (re)insurers on cyber risk underwriting, as they rely on existing guidelines and recommendations on risk management. Likewise, supervisory reporting on cyber underwriting is not yet widespread and comprehensive, even in jurisdictions with established regulatory reporting.

Identified challenges

The CUSG assessment sees the key challenges affecting cyber risk underwriting and relevant drivers as being the measurement of risk exposure and clarity of policies.

Measurement of risk exposure

Modelling cyber risk as an input for underwriting decisions remains underdeveloped, but the insurance industry continues to make progress in this area. The CUSG recognised that measuring cyber risk is inherently challenging, for a number of factors, and most notably for:

- evolving nature of cyber risk due to the expansion of digitalisation and interconnectedness (eg Internet of Things), the development of new attack and defence strategies as well as due to evolving legislative frameworks (eg data breach notification requirements), all of which makes historical data less relevant to project future cyber events and losses;
- limited loss experience and comparative shortage of reliable cyber risk data, partly due to limited disclosure of incidents and heterogeneity of data capture;
- difficulties in assessing policyholder vulnerabilities, given complexity of IT systems, security and risks and high specialisation needed for such assessment, certain reluctance to share information, and potential disproportionate costs of conducting cyber risk assessments compared to insurance premiums collected (particularly for small business customers);
- limited ability to take into account accumulation risk arising from concentration of IT services and software, interconnectedness of policyholders, and overlaps in coverage; and
- non-affirmative coverage of cyber risk create potential coverage uncertainties and challenges for insurers and supervisors in adequately measuring and assessing risk exposures. In addition, the challenges concerning measurement of risk exposures outlined in the preceding findings are compounded by the possibility of non-affirmative coverage.

Clarity of cyber insurance policies

While some issues (such as non-standardisation of policy wording) are to be expected regarding a relatively new and rapidly evolving line of business, other issues may have far-reaching implications. These may include the following:

- overlapping coverages in cyber insurance policies and other types of insurance policies, such as business interruption, ransomware, social engineering, and property damage;

- non-affirmative coverage issues as noted above; and
- treatment of ransoms, fines, terrorism and war risk, which raises other public policy issues (eg related to insurability of penalties and concerns about countering the financing of terrorism).

Supervisory considerations for fostering sustainable cyber risk underwriting

In view of these findings, the CUSG recognises the need for proactive supervisory attention to cyber insurance underwriting. To this end, the CUSG recommended to the IAIS' Executive Committee that the IAIS pursue a strategic approach focused on: (a) facilitating the monitoring, understanding and assessment of cyber risk underwriting exposure and impact; and (b) assisting supervisors in building relevant capacity to review cyber risk underwriting practices and exposure. This is aimed at achieving the following objectives:

Addressing non-affirmative cyber exposure

The IAIS should play an active role in encouraging supervisors to require improved clarity of policy coverage as regards cyber risk. The IAIS should monitor progress in addressing non-affirmative cover by insurers and supervisors and possibly set out further guidance.

Addressing heterogeneity in data capture (and facilitating data sharing initiatives)

The IAIS should monitor and analyse initiatives for developing a data taxonomy and will consider the potential for the IAIS to facilitate this work. Moreover, the IAIS should review current data sharing initiatives, with a view to identifying effective practices.

Addressing supervisory reporting on cyber exposure

The IAIS should further review current supervisory reporting practices and explore the utility of expanded supervisory reporting on cyber underwriting exposure. Moreover, consideration will be given to gathering cyber underwriting data to better understand total exposure as part of the Holistic Framework for Systemic Risk in the Insurance Sector.

Addressing risk measurement, including development of stress scenarios

The IAIS should review current industry and supervisory approaches relating to risk measurement, and initiatives for developing stress scenarios to estimate cyber underwriting exposure and will consider the potential for an IAIS role in furthering such work.

Addressing issues related to policy wording

The IAIS should analyse issues related to clarity of policy terms, conditions and exclusions with a view to encouraging convergence in understanding, although the CUSG concurs with stakeholders that compelled standardisation of policy wording should not presently be pursued.

Developing cyber awareness and expertise among supervisors

The IAIS should undertake initiatives to develop and share good practices on supervision of cyber underwriting.

Introduction

Although cyber risk is not new, its significance has grown in recent years, amplified by the evolution of technology and incidents such as NotPetya, WannaCry and other malware and data breaches. In 2019 the cost of cybersecurity and the average number of breaches increased by 12% and 11% respectively[2]. Costs may further rise as many jurisdictions are adapting and implementing data protection and privacy laws to protect individuals as well as introducing supervisory rules, guidance, and expectations for cyber security.

More recently, in response to the Covid-19 pandemic, many organisations and firms worldwide switched to large-scale remote work operations in the early months of 2020, and online traffic and business increased as a result of lock-downs, thereby highlighting the growing importance of the digital ecosystem while expanding opportunities for exploitation by cyber criminals and for other cyber incidents.[3]

Alongside the increase in cyber risk, the cyber insurance market has also grown significantly in recent years. Initially developed in the 1990's out of professional indemnity policies, many insurers now offer a form of cyber coverage, whether in a stand-alone policy or as an endorsement to an existing policy and for both first party and third party losses. Insurers have also integrated loss prevention tools to educate clients and further develop their resiliency against attacks and assist with recovery efforts.

Cyber insurance is expected to bring benefits in the form of greater policyholder awareness and stronger risk management practices, and its development will progressively help reduce the protection gap, thereby benefiting the economy at large.

From an insurance supervisory perspective however, the growth of cyber insurance has raised concerns, including questions on silent – or non-affirmative[4] –coverage as well as risk accumulation, with the potential for catastrophic loss across sectors.

Given this background, the IAIS included cyber risk underwriting among the strategic themes of its 2020-2024 Strategic Plan and Financial Outlook (SPFO), particularly under High Level Goal 1, which aims to assess and respond to issues that present opportunities, challenges and risks to the IAIS' mission.

Sources of information and approach to analysis

In preparing this report the CUSG carried out an extensive literature review and engaged both with Members and stakeholder representatives to form a broad informed view on the cyber insurance market, trends and initiatives as well as on the main challenges regarding cyber underwriting.

The material consulted during the literature review provided a broad overview of products, insurers' practices and known issues, as well as ongoing initiatives to address them (for

[2] Accenture and Ponemon Institute, "Cost Of Cyber Crime Study", October 2019.

[3] Marsh, "COVID-19: Cybersecurity Checklist for Remote Working", https://coronavirus.marsh.com/us/en/insights/research-and-briefings/covid-19-cybersecurity-remote-working.html

[4] "Coverage on a non-affirmative basis" refers to coverage for cyber-related losses under insurance policies with terms that neither explicitly encompass nor explicitly exclude coverage for cyber-related losses.

example, reports from the OECD[5], the Geneva Association[6] and International Institute of Finance[7]).

Data on the significance of cyber risk, the cyber insurance market and the potential impact of major cyber events on the insurance sector were collected from various public sources (privately-sponsored surveys and estimates, supervisory reports, table-top exercises), given the lack of widespread and comprehensive data registers in this area.

A stakeholder dialogue with industry participants in the last quarter of 2019 provided valuable insights with respect to the main challenges to cyber risk underwriting (eg applicant's risk assessment, terminology and exclusions), pricing and risk measurement, risk management as well as those arising from non-affirmative cyber cover. The stakeholder panel covered a range of participants (insurers, reinsurers, brokers, industry associations and professional consultancies) and geographies (Europe, North America and Asia).

Lastly, the IAIS conducted a stock-take on supervisory practices among its Members on supervisory approaches to cyber underwriting. Responses were submitted by seventeen IAIS Members distributed across main world regions and provided a broad view on regulatory reporting, supervisory guidelines on risk measurement and management as well as on supervisory capacity with respect to cyber risk underwriting.

The data and information collected has been key to forming the IAIS view on the main challenges facing cyber risk underwriting, both from an industry and supervisory perspective, and to outlining a supervisory approach to support the sustainable development of this line of business.

[5] OECD. (2017). *Enhancing the role of insurance in cyber risk management*. Retrieved from http://www.oecd.org/daf/fin/insurance/enhancing-the-role-of-insurance-in-cyber-risk-management-9789264282148-en.htm

[6] The Geneva Association. (2018). *Ten Key Questions on Cyber Risk and Cyber Risk Insurance.*

[7] Institute of International Finance (IIF). (2019). *Cyber Risk Insurance Update: Advances in Risk Management, Prioritisation, Prevention and Protection.*

1 Cyber insurance market

Cyber insurance is designed to provide first party and third party coverage to mitigate risk exposure by offsetting costs involved with recovery of cyber losses. Coverage may include losses from network security breaches, data and systems recovery costs, legal expenses and third-party indemnification related to data breaches, as well as business interruption costs.

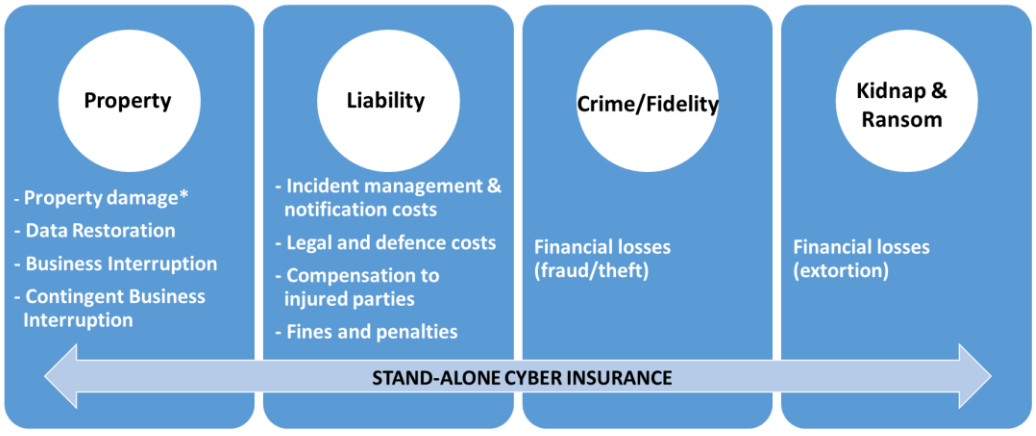
In recent years, the cyber insurance market has increased along with the frequency of cyber incidents and the scale of their damages. New data protection regulations require notifications to customers and, in the case of the financial sector, to supervisors. Cyber attacks could lead to severe damages to organisations, which in turn could suffer loss of customers, disruption of business, fines and a loss of intellectual property.

There is huge potential for further cyber insurance market development, based on estimates of the protection gap and increased cyber awareness. At the same time, there are some challenges (further examined in this report) that are holding back both the demand from prospective policyholders for cyber insurance and the appetite for insurers to underwrite cyber risk.

1.1 Products and services

The cyber insurance market has developed to provide financial protection for the digital security and privacy risks that have arisen as a result of increased reliance on digital technologies. The development of cyber insurance coverage has been driven by both the emergence of new risks and the application of exclusions in (traditional) property, liability and some specialty (eg crime, kidnap and ransom) policies (see Figure 1).

Figure 1: Losses and costs covered under cyber insurance policies



* Coverage for property damage provided in stand-alone cyber insurance policies is usually limited to damages to computer and/or other information technology equipment damaged as a result of a covered incident. At present, there is limited availability of broader property damage coverage under stand-alone cyber insurance policies

Note: Some of the costs identified above as liability costs (specifically incident management and notification costs and legal and defence costs) are actually first-party costs incurred by the insurer (rather than the reimbursement of costs incurred by a third-party as a result of a liability). However, they have been classified as such as they will generally only arise as a result of obligations to third parties. *Source*: Adapted from OECD (2020)[8]

[8] OECD (2020), *Encouraging Clarity in Cyber Insurance Coverage. The Role of Public Policy and Regulation*

The cyber insurance market is focused on protecting businesses[9] against the consequences of six main types of cyber incidents (from OECD, 2020[10]):

- data confidentiality breaches (including privacy breaches): where a company has allowed (or has not prevented) unauthorised access to the private information (financial, medical, biometric, commercial) of individuals or firms resulting in incident management and notification costs, data, software and hardware[11] restoration costs, legal and defence costs, compensation to injured parties and fines and penalties (regulatory and/or contractual);
- network security liability: where a company has allowed (or has not prevented) the use of its network in a cyber attack on a third party leading to legal and defence costs and compensation to injured parties;
- communication and media liability: where a company's digital communications activities (intentional or accidental) result in defamation, libel, slander or other harm to a third party leading to legal and defence costs and compensation to injured parties;
- technology disruptions: where a company's operations have been disrupted as the result of a technology failure (accidental or malicious) at the company or one of its service providers leading to business interruption losses (or contingent business interruption losses) and potentially data, software and hardware restoration costs;
- cyber extortion: where a company's ability to access its data (or network) has been compromised or breached as part of an extortion (ransomware) attempt, leading to incident management costs, financial losses (ransom payment) and/or business interruption and data, software and hardware restoration costs; and
- cyber fraud and theft: where a company's funds or assets are stolen or fraudulently expropriated, including through social engineering, resulting in financial losses.

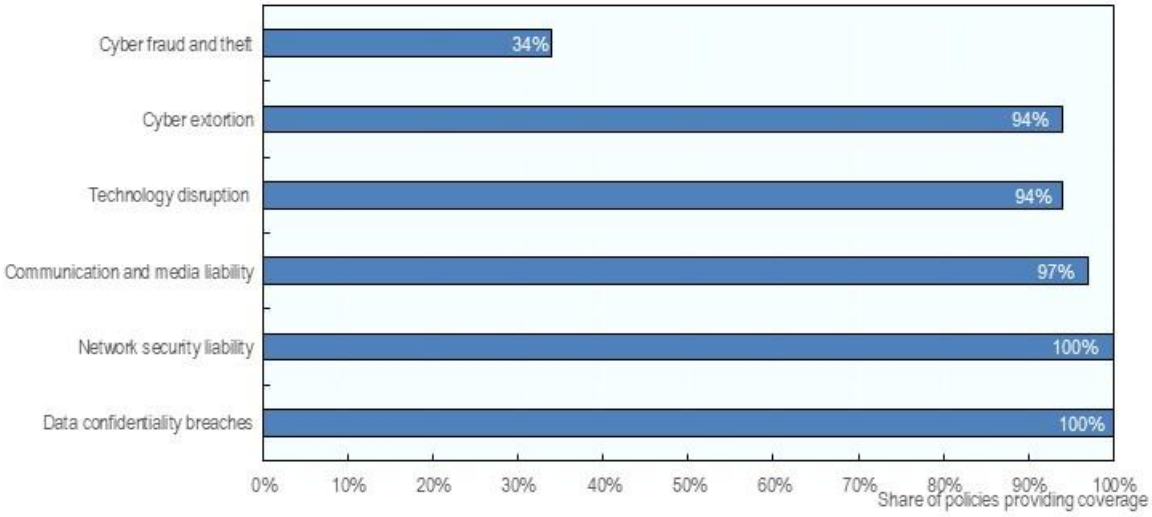
While the coverage offered in individual policies varies by insurer, an OECD review in 2019 of 35 publicly-available cyber insurance policies offered in Australia, Canada, Japan, Netherlands, United Kingdom, United States or offered on a regional (Europe) or global basis found coverage for many (but not all) of these types of incidents (see Figure 2).

[9] Insurers have also developed some cyber insurance coverage for individuals/households to protect against perils such as identity theft and ransomware or to cover liability related to cyber bullying. This coverage is often included in homeowner or civil liability insurance policies, although there is limited information available on the size of this market. In the United States, USD 9.3 million in premiums were reported for identity theft coverage in 2018 (NAIC, 2019).

[10] OECD (2020), *Encouraging Clarity in Cyber Insurance Coverage. The Role of Public Policy and Regulation.*

[11] While cyber insurance coverage does not generally reimburse losses related to physical damage, coverage for "bricked" devices (ie hardware rendered useless due to malware infection) is increasingly offered.

Figure 2: Types of incidents covered by cyber insurance policies



Source: OECD (2020).[12]

Insurance coverage for losses resulting from these types of cyber incidents may be provided as:

- stand-alone cyber insurance policies, specifically developed to address these types of risks;
- endorsements adding coverage for cyber incidents to other types of insurance policies (most commonly to property insurance policies, general liability/professional indemnity policies, crime/fidelity policies and kidnap and ransom policies[13]); and
- coverage for cyber incidents included in package policies (ie policies aimed at small businesses that package property and liability coverage).

Coverage that is explicitly provided, whether in stand-alone policies, through endorsements, or in package policies, is generally referred to as affirmative cyber insurance coverage (see section 2.1.5 for a discussion of non-affirmative cyber coverage).

In the United States, insurers are writing more stand-alone cyber insurance policies than package policies.[14] In Europe, stand-alone cyber insurance premiums accounted for 83% of cyber insurance premium reported to EIOPA in 2018 (with the rest written as endorsements).[15] In both the United States and Europe, the share of premium accounted for by stand-alone policies appears to have declined relative to 2016 although this may be partly due to better

[12] OECD (2020), *Encouraging Clarity in Cyber Insurance Coverage. The Role of Public Policy and Regulation*.

[13] Common examples include: business interruption coverage in property policies, financial loss coverage in crime/fidelity policies or legal defence and compensation cost coverage in general liability/professional indemnity policies.

[14] NAIC (2019), *Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement*, National Association of Insurance Commissioners, https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final%20%281%29.pdf.

[15] EIOPA (2019), *Cyber Risk for Insurers – Challenges and Opportunities*, European Insurance and Occupational Pensions Authority, https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf

reporting of cyber-related premiums written as part of package policies or as endorsements to other types of policies. A 2019 survey of brokers and underwriters from around the world, for example, identified a continuing trend towards acquiring cyber insurance coverage through stand-alone policies.[16]

Box 1: The role of cyber insurance in policyholders' cyber risk management

Similar to other lines of insurance business, cyber insurance can make an important contribution to improving policyholders' cyber risk management. Insurers (and intermediaries) can be important sources of advice on good cyber security practices and can encourage policyholders to improve their cyber security practices as part of the underwriting process. Where premium pricing is risk reflective (and subject to the measurement challenges discussed below), the premium rating could also provide an important incentive for policyholders to improve their cyber hygiene.

In addition to providing insurance coverage for cyber-related damages and losses, many cyber insurers offer various risk mitigation and crisis response services to policyholders (often through third party suppliers), ranging from cyber security services such as vulnerability scanning and penetration tests to post-incident response services such as data and system restoration to legal and public relations advice. There is some evidence that these services are valued by policyholders and may reduce the ultimate cost of a cyber incident for the policyholder and the insurer.[17]

1.2 Size of market

Very few statistical agencies or insurance supervisors collect regular data on cyber insurance as a specific class of business separate from data on other classes of business (with the exception of the NAIC in the United States, see 3. 1.1). As a result, most estimates of the size of the cyber insurance market globally or for individual countries are provided by private firms and will normally only capture affirmative cyber insurance coverage or only stand-alone cyber insurance coverage.

Most estimates suggest written premiums for cyber insurance of approximately USD 4-5 billion globally in 2018:

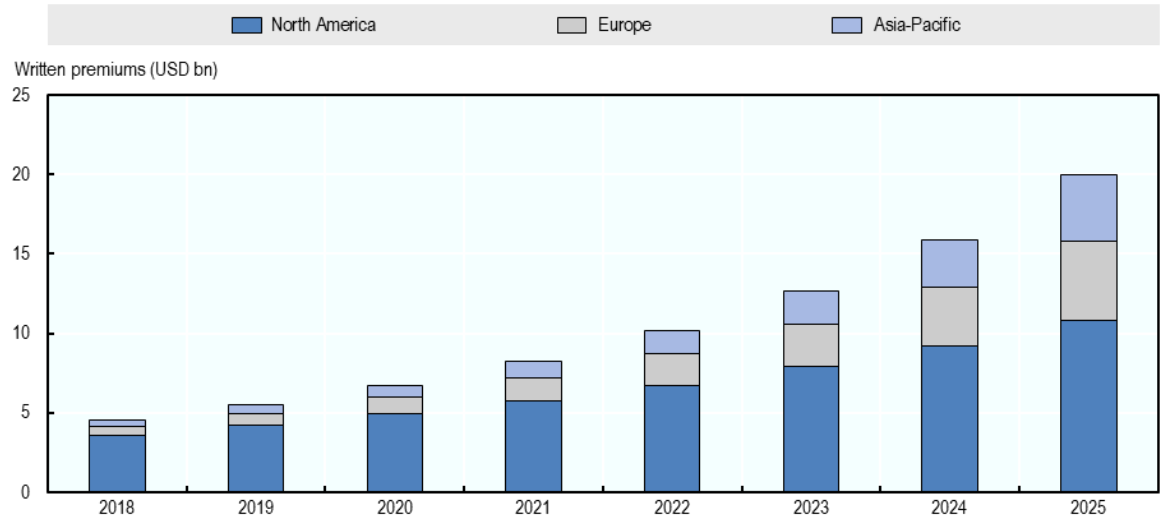
- North America: The NAIC estimated that admitted and surplus lines insurers in the United States wrote USD 3.6 billion in cyber insurance premium for stand-alone and package policies in 2018.[18] This is consistent with estimates by Munich Re[19] of written premiums of approximately USD 3.6 billion in 2018 for all of North America. According

[16] Partner Re and Advisen (2019), *Cyber Insurance – The Market's View*, Partner Re and Advisen, https://partnerre.com/wp-content/uploads/2019/10/Cyber_Insurance_The_Markets_View_2019-1.pdf.
[17] OECD (2017), *Enhancing the role of insurance in cyber risk management*, OECD, http://www.oecd.org/daf/fin/insurance/enhancing-the-role-of-insurance-in-cyber-risk-management-9789264282148-en.htm.
[18] NAIC (2019), *Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement*, National Association of Insurance Commissioners, https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final%20%281%29.pdf.
[19] Reported in Faulkner, M. (2019), "Europe and Asia cyber premiums to outpace US growth", *Insurance Day*, 21 October 2019, https://insuranceday.maritimeintelligence.informa.com/ID1129477/Europe-and-Asia-cyber-premiums-to-outpace-US-growth (2018 estimates derived based on reported growth rates).

to Munich Re, North America accounts for approximately 80% of cyber insurance premium.[20] Moreover, over 80% of the cyber insurance market is being written by the top twenty insurers.

- Cyber insurance premium is expected to grow rapidly in the coming years, particularly in Europe: Large (re)insurance groups in Europe[21] reported EUR 295 million in cyber insurance written premium in 2018 in responses to an EIOPA questionnaire on cyber risk.[22] This estimate is lower than estimates made by the expert team (approximately USD 550 million) extrapolating Munich Re long-term projections.
- Asia-Pacific: The expert group did not find any available data on cyber insurance premiums from insurance supervisors in the Asia-Pacific region. Extrapolating Munich Re estimates, the cyber insurance written premium in Asia-Pacific would amount to approximately USD 380 million. Aon estimates approximately AUD 60-100 million in cyber insurance written premium in Australia. [23]

Figure 3: Projected growth in cyber insurance market (2018-2025)



Note: The chart assumes constant annual growth rates based on Munich Re estimates of annual growth rates over the period. *Source:* IAIS calculations based on Munich Re

[20] Munich Re (2018), *Cyber insurance market outlook*, https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-market-outlook-2018.html
[21] Responses to the EIOPA questionnaire were received from 41 large (re)insurance groups based in 12 European countries that together account for approximately 75% of consolidated insurance market assets.
[22] EIOPA (2019), *Cyber Risk for Insurers – Challenges and Opportunities*, European Insurance and Occupational Pensions Authority, https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf
[23] Aon (2018), Cyber Insurance Market Insights - Q3 2018, http://aoninsights.com.au/wp-content/uploads/Aon-Cyber-Insurance-Market-Insights-Article.pdf and Aon (2019), Cyber Insurance Market Insights – Q4 2019, https://aoninsights.com.au/cyber-insurance-market-insights-q4-2019/.

1.2.1 *Cyber insurance as a fraction of the overall insurance market*

Despite the growth in premium volume, the affirmative cyber insurance market remains small relative to other commercial insurance business lines – at approximately 1.7% of the size of the property insurance market and 2.9% of the general liability insurance market in 2018.[24]

1.2.2 *Cyber insurance take-up rates and limits*

Data on cyber insurance take-up rates is published by a number of organisations based on survey data and appears to show a much more limited take-up of cyber insurance relative to other commercial insurance lines. For example:

- Based on a survey of cyber security professional in Belgium, France, Germany, Spain, Netherlands, United Kingdom and the United States at the end of 2018, Hiscox found that 41% of surveyed firms had adopted cyber insurance.[25]
- The US Council of Insurance Agents and Brokers, which conducts regular surveys of its intermediary members on cyber insurance take-up and challenges, found an overall take-up rate of 33% of US businesses at the end of 2018.26 This is consistent with an estimate of take-up of cyber insurance of 38% by Marsh among its US-based clients.[27]
- Insurance firms and intermediaries in Australia estimated that take-up rates in early 2019 were approximately 20% overall (and 35% among larger firms).[28]

One survey, undertaken at the end of 2017, provided a breakdown by country and company size and identified a significant gap between the share of larger firms that have cyber insurance (49% to 62%, depending on the country) relative to the share of smaller firms (20% to 33%).[29]

Some limited data is also available for the take-up of cyber insurance by sector. Among Marsh clients in the United States, take-up of cyber insurance is highest in the education, health care, hospitality and gaming and communications, media and technology sectors (ranging from 50% take-up to close to 70%). Take-up of cyber insurance is much lower among financial institutions (less than 30%) and in the manufacturing sector (approximately 30%).

[24] https://stats.oecd.org/Index.aspx?DatasetCode=INSIND. OECD figures on the property insurance market include both residential and commercial property insurance premiums. In the OECD insurance statistics exercise, cyber insurance is not reported as a separate line of business and therefore premiums collected for cyber insurance may be included in general liability (or other classes of business) premiums reported to the OECD.

[25] Hiscox (2019), *Hiscox Cyber Readiness Report 2019*, Hiscox, https://www.hiscox.com/sites/default/files/content/documents/2019-Hiscox-Cyber-Readiness-Report.pdf

[26] CIAB (2019), *Cyber Insurance Market Watch Survey: Executive Summary (Fall 2018),* The Council of Insurance Agents and Brokers, https://www.ciab.com/download/16876.

[27] Marsh (2019), *2018 Cyber Insurance Trends: Purchasing, Limits and Pricing*, Marsh & McLennan Companies, https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/cyber-insurance-trends-report-2018.pdf.

[28] OECD (2020), *Insurance Coverage for Cyber Terrorism in Australia*, OECD and ARPC.

[29] Hiscox (2018), *Hiscox Cyber Readiness Report 2018*, Hiscox, https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf.

Based on input from the roundtable discussions with industry participants, insurers' risk appetite is limited in terms of exposure to single customers and to applicants with significant cyber incident history, who in some cases could see their applications rejected. On average, insurers stated that cyber cover offers are limited to USD/EUR 25m, with higher limits for larger customers (eg USD/EUR 100m) and towers (of up to USD/EUR 500/600m) available.

Typical cyber insurance policy limits in the United States are estimated to be less than or equal to USD 5 million, with an average of approximately USD 2.8 million.[30]

1.2.3 *Cyber insurance vs cyber losses*

Estimates of the cost of cyber incidents are orders of magnitude above the amount of losses absorbed by the insurance sector, which suggests a significant protection gap and large potential for market growth. For example, the most recent study by Accenture on the cost of cybercrime estimates that the annual cost to the average company of cybercrime (a sub-set of all cyber incidents) reached USD 13.0 million in 2018 (or a total of USD 4.6 billion for the 355 firms covered in the survey).[31] The average cost of a data breach (a sub-set of cyber incidents) reached USD 3.92 million in 2018.[32] By contrast, the average claim paid by US admitted insurers in 2018 was approximately USD 146,000.[33] An estimate by PCS (a loss data aggregation provider) suggests that less than 15% of the major losses suffered by Equifax (data breach) and Merck, Maersk and FedEx (ransomware) in 2017 were covered by insurance.[34]

The Center for Strategic & International Studies (CSIS) and McAfee estimated the global annual cost due to cybercrimes as high as USD 600 billion.[35]

1.2.4 *Pricing and underwriting performance*

As a result of the exposure measurement challenges outlined below, there are opposing views on whether current pricing levels are above or below the fair price. Some insurers worry that current premium rates are not actuarially sustainable. Others think that the opposite is true. This view is supported by the Lloyd's Market Association statistics covering 2013-2016, showing a gross loss ratio of cyber risk policies comfortably below 70%. In the United States, cyber insurance has generally been a profitable line of business with low loss (and combined)

[30] CIAB.com/resources/cyber-insurance-by-the-numbers
[31] Accenture and Ponemon Institute (2019), *Ninth Annual Cost of Cybercrime Study*, Accenture, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50. The Accenture report is based on interviews of 355 (mostly larger) companies in 11 countries.
[32] IBM Security and Ponemon Institute (2019), Cost of a Data Breach Report: 2019, IBM Security, https://www.ibm.com/security/data-breach. The IBM Security report is based on interviews of 500 companies around the world that experienced a data breach in 2017-2018.
[33] Data provided by NAIC based on figures reported for the 2019 *Cybersecurity Insurance and Identity Theft Coverage Supplement*. The average is calculated based only on claims closed with a payment made.
[34] Johansmeyer, T. (2018), "Short-Term, Short-Tail", presented at the OECD Conference on Unleashing the Potential of the Cyber Insurance Market (22-23 February 2015, Paris), https://www.oecd.org/daf/fin/insurance/Presentations-Conference-cyber-insurance-market.pdf.
[35] CSIS and McAfee, "Economic Impact of Cybercrime— No Slowing Down", February 2018.

ratios – although with significant variation across insurers.[36] AM Best estimates that the direct paid loss ratio for US cyber insurers was below 30% in 2015, 2016, 2017 and 2018 (for both stand-alone and packaged policies).[37] However, Munich Re has estimated more recently that loss ratios in cyber insurance may be as high as 80% (cf fn 19).

The market appears to be fairly competitive, leading to price competition among insurers (supported by low loss ratios in recent years). However, feedback from industry noted a recent increase in premium rates driven by a higher frequency of ransomware attacks and more significant ransoms demands.[38]

1.3 Cyber reinsurance

According to estimates from Swiss Re[39], around 40% of cyber risk premiums are ceded to reinsurers compared to 10%-15% for more mature lines of business, which may suggest that insurers have limited appetite for retaining cyber risk and/or are using reinsurance as a means to capture market share. Swiss Re estimates that 95% of premiums for cyber risk ceded to reinsurers are ceded under standalone cyber reinsurance treaties (ie only a small amount of coverage for cyber risk in package policies or other lines of business is ceded to reinsurers). An alternative reinsurance market (ie alternative risk transfer to capital markets) has yet to emerge for cyber risks, with a few exceptions.[40]

Swiss Re estimates current reinsurance capacity at USD 1.5billion, although warns that in the case of large loss events (eg triggering contingent business interruption), the market capacity may reduce given the high concentration of the market, with the top 10 carriers writing half of the global premium.

Reinsurers reportedly have a preference for assuming risk on a proportional basis, potentially due to concerns about assuming the accumulation (tail) risk that would result from non-proportional (excess-of-loss) reinsurance arrangements. According to Swiss Re, there is an increasing demand for non-proportional reinsurance with attachment points ranging from 90% to 200% loss ratios.[41] This was confirmed by insurers participating in the IAIS-industry roundtables.

[36] For example, the top 20 providers of stand-alone insurance coverage in the United States reported loss ratios in 2018 that ranged from 0.03% to 82.7% (NAIC, 2019).
[37] AM Best (2019), *Cyber Insurers are Profitable Today, but wary of Tomorrow's Risks*, AM Best, http://www3.ambest.com/bestweekpdfs/sr507453119175full.pdf.
[38] https://www.cpomagazine.com/cyber-security/ransomware-attacks-are-causing-cyber-insurance-rates-to-go-through-the-roof-premiums-up-as-much-as-25-percent/
[39] Swiss Re "Could cyber risk be a growth engine for reinsurance?", August 2019, https://www.swissre.com/reinsurance/property-and-casualty/reinsurance/cyber-reinsurance/reinsurance-a-growth-engine-for-cyber.html.
[40] For example, one insurance-linked security has been issued to provide coverage for a cloud service outage (Evans, S., "Hiscox backs PCS trigger parametric cyber risk transfer on AkinovA", Artemis, 9 January 2020, https://www.artemis.bm/news/hiscox-backs-pcs-trigger-parametric-cyber-risk-transfer-on-akinova/).
[41] Swiss Re, see above.

2 Key findings from literature review and stakeholder engagement

The following section provide the results of the CUSG's review of relevant literature and from its discussions with targeted stakeholders at the roundtables held in Basel in October 2019 and Washington DC in November 2019.

2.1 Measurement of risk exposure

One of the most important challenges identified in underwriting cyber insurance relates to the ability of insurers to measure their exposure to underwritten cyber risk. Measuring cyber risk is critical for sustainable pricing of cyber insurance, allowing for sufficient premium income to cover expected losses and capital remuneration in addition to operational costs and commercial margins. It is also key to inform the amount of capital that insurers should set aside in order to protect themselves from unexpected losses and to help define risk management approaches, including coverage offered, retained and transferred to reinsurance markets.

Based on information gathered during the industry roundtables and confirmed by literature, current quantitative approaches to cyber risk measurement[42] include actuarial approaches, scenario analyses and combinations of both.[43] General feedback from the roundtables indicated a degree of model risk in current approaches for cyber risk estimates. According to industry participants, while cyber risk modelling is becoming more sophisticated, there is significant variability in the estimates produced by different vendor models, which undermines their use as sole source for pricing and more advanced risk management. Common practices adopted see a combination of various vendor models, along with scenario analysis and expert judgement.

Based on the review of literature on this topic and the roundtable discussions, five main challenges to cyber risk measurement have been identified: (i) the evolving nature of cyber risk; (ii) limited cyber loss experience; (iii) difficulties in assessing policyholder vulnerabilities; (iv) accumulation risk; and (v) non-affirmative exposure.

[42] According to a SANS Institute survey on 194 US insurers, about 58% of respondents declared using quantitative approaches (of which 35% use not very detailed models), *Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey,* 2016.
[43] Swiss Re Institute, *Cyber: getting to grips with a complex risk,* 2017.

2.1.1 *Evolving nature of cyber risk*

Cyber risk is an enormous challenge that continues to grow at an exponential rate. With the advent of new cyber threats developing daily, changes in the cyber risk landscape and the balance between attackers and defenders could affect the frequency and/or severity of cyber loss probability distributions.[44]

Measuring cyber risk using only historical data could lead to underestimation (or overestimation) of future losses related to cyber insurance.

2.1.1.1 Increasing digitalisation and interconnectedness

The emergence and growth of cyber risk exposure has been driven, in the first instance, by the increasing reliance on data and technology in the operations of policyholders. Digitisation and electronic data processing has made data an increasingly critical asset for firms to design, develop and distribute their products and services. Operational technologies, including the Internet of Things (IoT), and remote controls are playing an increasing role in executing business and production processes (sometimes) autonomously. In addition, many of these data and technologies are connected, increasing the potential vulnerability, individually or at an aggregate level, without adequate assurance that systems and data dependency is clearly and fully recognised. The ever increasing reliance on data, software and hardware amplifies the value of these assets to businesses and the consequences of a loss or disruption as a result of a cyber-attack or IT failure.

2.1.1.2 Evolving threats and defences

Both the literature review and the input from the roundtable participants point to challenges created by the evolving nature of cyber threats and defences. The methods used by the perpetrators of cyber-attacks – and the processes implemented by policyholders (and their service providers) to protect against these attacks – are continuously evolving. Information on past threats or effective protection methods may become ineffective if new threats in new environments show little resemblance to past threats.

2.1.1.3 Evolving legislative frameworks

The legislative and regulatory frameworks that establish firms' privacy and cyber security obligations towards their employees, customers and shareholders – and which drive many of the third party/liability losses covered in cyber insurance policies – are relatively new, evolving and can be significantly different from one jurisdiction to another. As a result, the exposure of insurers to the liability-related losses of their policyholders is frequently changing and subject to uncertainty.

2.1.2 *Limited loss experience*

Loss experience on past incidents plays a critical role in underwriting insurance coverage in most lines of business. However, data on loss experience resulting from cyber incidents is not always readily available, and a number of challenges impede the availability of this data.

Lack of, incompleteness or inaccuracy of historical data decreases the statistical reliability of actuarial models' distribution parameters and increases the uncertainty around loss

[44] As an example, one potential major vulnerability in the future may arise from the adoption of quantum computing, which could make existing encryption techniques outdated and easier to hack.

estimates.[45] Moreover, as revealed by roundtable discussions, insurers tend to rely on data on cyber insurance claims, which are only a fraction of total cyber incidents given the low take-up rates of cyber insurance and that not all incidents generate claims.

2.1.2.1 Cyber is an emerging risk

Cyber risk is (still) a relatively new (and constantly evolving) risk for insurers, which means that historical data on past cyber losses and cyber incidents is limited. As a result, it is difficult to develop statistically robust models for pricing and risk management.

2.1.2.2 Limited disclosure of incidents

A major driver of data scarcity is that firms can be reluctant to report incidents following an attack because of potential reputational and economic implications. Not all cyber incidents are disclosed, unless it is mandatory in the jurisdiction or for specific sectors. Where reporting is mandatory, relevant data may not be publicly disclosed or shared with interested parties. Roundtable participants pointed out that there is uncertainty on whether insureds need to report incidents that do not give rise to claims.

2.1.2.3 Heterogeneity of data capture

The comparability (and ultimate utility) of the incident data that is available is limited by a lack of a shared taxonomy for categorising the incidents and resulting losses (see box below), thereby increasing the uncertainty around loss estimates. Lack of a harmonised taxonomy for cyber risk and the different extent and nature of data collected (eg direct financial losses, legal expenses, fines, time to recovery, cause, etc.) add to the above challenges. These shortcomings undermine the possibility of combining internal and external data (eg consortium data, public data, or claims data following a merger with another insurer) and forming a consistent view of cyber risk when accessing external or public data.

Box 2: Considerations on data collection

There are broadly four options for improving data availability. In order of increasing ambition, they are: (i) (extension of) a lexicon of cyber insurance terms; (ii) a data taxonomy for the classification of events; (iii) a detailed technical framework; and (iv) seeking to facilitate a data sharing initiative.

i. Lexicon

A lexicon setting out standardised definitions of terms related to cyber insurance would constitute a modest step towards greater convergence in cyber risk measurement. An example is the 'Cyber Lexicon' published by the Financial Stability Board (FSB)[46]. This lexicon was developed to support the work of the FSB and standard setting bodies specifically for the financial sector. It is not intended for legal interpretations in international or private agreements and contracts. In developing the lexicon, the FSB consulted with other organisations that are active in the establishment of cyber security standards. These are the ISO, ISACA, the SANS Institute and NIST, all of which have developed their own cyber lexicon.

[45] Biener, Eling Wirfs,"Insurability of cyber risk: an empirical analysis", University of St. Gallen 2015.
[46] Financial Stability Board "Cyber Lexicon", November 2018, https://www.fsb.org/2018/11/cyber-lexicon/.

ii. Data taxonomy

While a lexicon is limited to the standardisation of particular terms, a data taxonomy would further set out a standardised set of data attributes to capture for cyber risk events and/or exposures. An example of this is the trial performed by the CRO Forum[47] within its membership on the creation of a common categorisation methodology for cyber events. In this trial, there are eighteen attributes to describe each cyber event, with further categories within each attribute for further delineation. Examples of attributes are event type, discovery method, asset and financial impact. The categories under the 'discovery method' attribute for example are audit, security control, third party, user, monitoring service, attacker, other and unknown. For each category, the taxonomy offers a description and examples where relevant. Other comparable taxonomies are three industry standard taxonomies: VERIS[48], STIX[49] and ENISA Threat Taxonomy.[50] Whilst the intents of each taxonomy are similar, they differ in scope of events captured, and breadth and depth of categorisation.

Another example of this type of taxonomy is the Cybersecurity Incident Taxonomy published by the European Union's NIS Cooperation Group in July 2018.[51] This taxonomy focuses on large-scale cybersecurity incidents requiring EU cooperation. The structure of this taxonomy is less granular than the CRO Forum trial. The taxonomy is structured into two core parts: nature of the incident (ie root cause and severity) and impact (ie sector impacted, scale of impact, and outlook).

iii. Detailed threat technical framework

A technical framework would go a step further in that it would introduce a time dimension to the description of events. In the more basic taxonomy, each event has a point in time classification, typically done after the event, which does not capture the evolution of the risk as the event unfolds. In other words, the basic taxonomy focuses on the 'what', and the technical taxonomy goes into the 'how' at various attack stages.

An example of a detailed technical framework is the MITRE ATT&CK (MITRE's Adversarial Tactics, Techniques, and Common Knowledge)[52]. MITRE ATT&CK is a globally accessible knowledge base that systematically categorises the various phases of an adversary's attack lifecycle and the platforms they are known to target. The taxonomy is structured into tactics (motivation of attack) and techniques (methodology of attack) under each tactic. A description of each technique is also given. For example, under the 'Initial Access' Tactic for attacking enterprises, there are definitions for eleven different techniques for access like spearphishing link, trusted relationship and valid accounts. Other examples of enterprise tactics are execution, discovery, lateral movement and impact. ATT&CK provides a common language to structure, compare and analyse cyber threats.

[47] CRO Forum, "Supporting on-going capture and sharing of digital event data", February 2018.
[48] http://veriscommunity.net/
[49] https://oasis-open.github.io/cti-documentation/stix/intro
[50] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/at_download/file
[51] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53646
[52] https://attack.mitre.org/

iv Data sharing initiative

A data sharing initiative would be the most ambitious option. It would be predicated on information being collected using a consistent system of classification.

According to an OECD report[53], data sharing initiatives have typically been led by industry bodies and insurance associations, rather than by regulators or supervisors, with some more broadly focussed on improving risk management. The aforementioned CRO Forum trial is an example where member (re)insurers share anonymous incidents information based on a shared taxonomy. Other data sharing initiatives have been emerging in various jurisdictions.[54]

The first loss database was set up by NetDiligence in 2014 in the United States. Since then they have been publishing an annual Cyber Claims Study. In 2019, the report[55] features analysis of 2,081 claims arising from events from 2014-2018. The claims data has been aggregated in over 20 attributes, including total, average, and median costs (total breach, crisis services, legal and regulatory, and per-record); the nature of the event (type of data exposed, business sectors affected, revenue size of claimants, causes of loss); and the financial impact of cybercrimes (business interruption, malicious insiders, social engineering, ransomware)[56].

2.1.3 *Difficulties in assessing policyholder vulnerabilities*

Developing an accurate assessment of a policyholder's cyber risk exposure is a challenging process.

As a result (according to roundtables participants), assessment of policyholders' cyber risk is much more focussed on governance and process, unlike in some other lines of business, where a technical/engineering assessment is a significant component of underwriting approaches (such as property insurance).

2.1.3.1 Complicated to understand policyholder systems and risks

Understanding the effectiveness of a policyholder's cyber security is complex and depends on multiple elements and how they work together (software patching policy, cyber risk education, privilege management, firewalls, vulnerability monitoring, event logs analysis, disaster recovery and back-up system, data management, connected devices, etc.).

Risk assessment is normally based on policyholder-questionnaires and inside-out vulnerability scans.[57]

[53] OECD, "The role of public policy and regulation in enhancing the availability of data for cyber insurance underwriting", 2020.

[54] For example, The Association of British Insurers has been asking the Information Commissioner's Office (ICO) to make anonymised cyber breach data publicly available. Similar recommendations have also been voiced by other organisations globally, eg The Insurance Council of New Zealand and European Insurance and Occupational Pensions Authority (EIOPA). The Bank of England has also committed to work with HM Treasury and other authorities to encourage greater cyber risk data sharing.

[55] NetDiligence, "Cyber Claims Study", 2019.

[56] The NetDiligence Cyber Claims Study compiles data from various sources: structured interviews with IICTF members who represent cyber insurers, incident response organisations, specialist legal advisors, and cyber technologists.

[57] For example, the RMS model takes into consideration an assessment of threat-actor groups, human vulnerabilities, digital assets at risk, outside-in vulnerabilities, historical cyber incidents, loss process

Different understandings of complex technical elements between policyholders and insurers can complicate the collection and interpretation of cyber security information. For instance, it can be difficult to get consistent responses to underwriting questions regarding the presence of firewall or password conventions.

While some objective indicators (such as the nature of data managed, revenues, number of (IT) staff, main cloud provider, industry, geographical location, etc.) may provide useful information to identify possible threats as well as loss impacts and some correlation measures, self-assessment questionnaires and inside-out scan assessment of policyholders' networks[58] (the toolkit normally used in case of Small and Medium Enterprise (SME) customers) are unlikely to provide a reliable and comprehensive view of the vulnerabilities to which insureds may be exposed.

Deeper assessments conducted on larger customers by way of dedicated meetings with key policyholder staff (eg CIO, CISO, etc.) might provide further insight, particularly from the governance perspective; however, even in these cases, insurers may not be able to obtain a full picture of customers' cyber risk exposure and posture.

In addition, the internal cyber security posture of an organisation is not enough to protect it from cyber risks. Most of, if not all, organisations rely on outsourcing specific functions and services to specialised providers. Low security posture and security failures of third parties could disrupt operations of client organisations, leading to business interruptions, data breaches and/or data losses with potential severe financial, operational and reputational consequences. The longer the supply chain and the more entities involved, the higher are (direct and indirect) cyber risks.

Box 3: Cloud computing[59]

An area where outsourcing is becoming increasingly popular is cloud services. In addition to providing enhanced computational and storage capacity, cloud service providers generally feature higher security standards, technology, infrastructure and skills that would not be possible to maintain by most organisations. To achieve these standards, cloud services providers critically rely on scale economies. While switching to the cloud could increase security, at the same time, this could create single points of failure and cyber risk concentration of a systemic scale. Moreover, cloud services (eg IaaS, PaaS, SaaS) differ with respect to the split of security responsibilities between providers and customers.

2.1.3.2 Policyholder reluctance to share information

As in other lines of business, insurers may face challenges in collecting accurate and complete information from policyholders. Policyholders may be reluctant to complete all answers in questionnaires or to provide the access requested by insurers to gather information. Though generally of a better quality for larger covers, underwriting and exposure data is consequently seldom complete. Responses can also be difficult to interpret or may be overly cautious where clients are concerned about possible non-disclosure or inaccurate information leading to

footprints, and the interplay with insurance contract terms – including reinsurance terms and conditions (https://www.rms.com/models/cyber).

[58] For example, FICO Cyber risk score and BitSight security ratings provide security scores based on scan of the IP address and externally observable data and benchmark outcomes with known vulnerabilities.

[59] For more details see Financial Stability Board, "Third-party dependencies in cloud services", December 2019.

claims being rejected. Clients are reluctant to provide the level of insight into their internal processes that insurers would like to receive for their assessment. Some clients even restrict access to interviews. These challenges are exacerbated by the sensitive nature of cyber security information.

2.1.3.3 Insufficient technical expertise

A lack of cyber expertise applies to both underwriters and policyholders. Arguably, with better understanding, policyholders would be more confident in providing information to help the underwriting process. The Global Federation of Insurance Associations (GFIA)[60] identified that underwriters are not always cyber security experts, so some insurers use internal or external experts to assist in the underwriting process. GFIA also noted that consumer education is critical with respect to this emerging risk and that consumers and insurers/brokers need to collaborate in the gap analysis to understand policy coverage requirements. The lack of expertise is closely linked to the lack of experience. Due to the infancy of this class of business, there are a lot of first time buyers.[61] Therefore, it is hard for clients to determine how much risk to transfer; and insurers are also faced with risks they may have never previously quantified.

2.1.3.4 Cost effectiveness issues

Because of the above challenges in assessing the cyber security posture of policyholders, insurers must invest significant resources in cyber underwriting. For the SME market, the level of premiums may not always be significant enough to justify an investment in underwriting. Roundtable participants indicated that they often make use of more simplified underwriting approaches, such as limits and portfolio diversification, to manage SME cyber risk exposure rather than more sophisticated assessments of individual policyholders.

2.1.4 *Accumulation risk*

For insurers and (more importantly) for reinsurers, accumulation risk is one of the most significant challenges. According to CRO Forum, accumulation risk *"originates from the concentration of insured risks or coverages that may be affected by events or circumstances that cause substantial losses under several insurance policies, and potentially over multiple years and geographies.*[62] Cyber risk accumulations may arise from the emergence of a vulnerability at (or in the products offered by) a common information technology service provider or due to the interconnectedness of information technology systems and policyholders. A cyber incident could also trigger losses across multiple policies given the overlaps in coverage for cyber risks and the potential for non-affirmative exposure.[63]

2.1.4.1 Concentration of IT services

Accumulation risk may arise from shared software or hardware vulnerabilities, disruption/outages of critical information technology services and/or failures affecting critical

[60] GFIA Observations on Cybersecurity, February 2018.
[61] Ulrik Franke, "The cyber insurance market in Sweden", Science Direct, April 2017.
[62] CRO forum, "Casualty Accumulation Risk" 2015.
[63] As outlined below, various non-life insurance policies might provide some cyber coverage. For example general liability, D&O or E&O policies in the case of third-party liabilities following data breaches, property insurance in the case of cyber incidents leading to property damages or (contingent) business interruption. This source of accumulation risk can sometimes be hidden, due to unclear policy wording regarding a cyber exclusion, or being silent (ie non-affirmative cyber).

infrastructure, such as the power supply or telecommunications networks[64] (although insurers often apply exclusions to disruptions of critical utility services). High levels of concentration in the use of certain software and operating systems (eg Windows or IOS), hardware (eg central processing units), cloud services providers (eg Amazon, Google, Microsoft, IBM, etc.) and platforms exacerbate the potential for accumulation risk to arise. For example, a security incident at a cloud provider may involve multiple policyholders at the same time, increasing the accumulation of cyber losses for insurers offering (contingent) business interruption coverage.

Such a characteristic makes cyber accumulation risk different from (and potentially more worrisome than) other insured perils, since the degree of diversification that insurers can achieve by building large and geographically diverse cyber risk insurance portfolios is limited.

2.1.4.2 Interconnectedness

The increase in devices connected to the internet allows for the simultaneous exploitation of vulnerabilities in common IT products and services on a widespread basis, while some forms of malware have been designed to exploit the connection between systems to spread across networks and therefore policyholders. This creates the potential for correlated losses across many policyholders based on these types of interconnections.[65]

2.1.5 *Non-affirmative exposure*

The subject of "non-affirmative coverage" is prominently featured in the literature and was addressed with stakeholders during the roundtable sessions. For purposes of this paper, the IAIS understands "coverage on an affirmative basis" to mean coverage for cyber-related losses under insurance policies with terms that explicitly encompass coverage for cyber-related losses. "Coverage on a non-affirmative basis," on the other hand, refers to coverage for cyber-related losses under insurance policies with terms that neither explicitly encompass nor explicitly exclude coverage for cyber-related losses.[66]

In the responses to the stock-take (see Section 3), supervisory authorities expressed concern about non-affirmative coverage, which presents insurers with the possibility of losses – and, in the worst case, the accumulation of losses – for which the insurers have not collected any premium.

In general, roundtable participants identified the issue of non-affirmative coverage as one of the main challenges for insurers. To this end, some major insurers have taken steps toward

[64] OECD, "Enhancing the Role of Insurance in Cyber Risk Management", 2017.
[65] Swiss Re "Cyber risks in an interconnected world", November 2017.
[66] One clear message from the IAIS-industry roundtable participants, however, was that there is not agreement among stakeholders as to the definition of non-affirmative (or "silent") cyber coverage.

comprehensively writing cyber insurance only on an affirmative basis.[67,68] As an industry, that process is not complete[69], but roundtable participants were in agreement that the industry itself is addressing the issue through clearer cyber exclusions in non-cyber policies, together with cyber endorsements and stand-alone cyber products. That being said, an unresolved issue highlighted by roundtable participants is that of distinguishing the dividing line between what is a cyber-exposure/loss and what is not – particularly as regards certain physical losses that may arise under a property insurance policy (see 2.2.1 on overlapping coverage).

Box 4: Scenario analysis

Scenario analysis is often used to estimate potential cyber losses under historical or expertly-designed scenarios, which is particularly useful in case of lack of data or when past data are not suitable to model future losses.

Scenario analysis is applied particularly for assessing accumulation risk or Probable Maximum Losses (PML).[70] One possible application of scenario analysis is the assessment of losses arising from non-affirmative cyber cover, by simulating the trigger of property and liability insurances potentially affected by this issue.

In contrast to actuarial approaches, scenario analysis generally provides point estimates of losses under the assumption that a given scenario will happen; however, this is sometimes counterbalanced by varying the severity of a specific scenario, for example with respect to the length of the recovery process[71] or by estimating the variability of the impact by relaxing some of the assumptions or by introducing stochastic modelling of some risk factors[72].

Scenario analysis applied to accumulation risk generally requires detailed and large information and data sets to estimate the share of the insured portfolio affected, the damage suffered as well as the insurance policies triggered.

For example, in case of accumulation risk scenarios involving the failure of critical vendors (eg cloud services or power suppliers), impact estimates may require information (or assumptions)

[67] For example, as noted by OECD (2020) in "Encouraging Clarity in Cyber Insurance Coverage. The Role of Public Policy and Regulation": *In the Lloyd's market, all first party property damage policies that renew after 1 January 2020 will need to either provide affirmative coverage for – or exclude – cyber risks (and the same will apply to liability lines and treaty reinsurance at a later date) (Faulkner, 2019). AIG has committed to provide affirmative coverage or apply exclusions for physical and non-physical cyber risks across almost all commercial property and liability lines by January 2020 (Carrier Management, 2019). Allianz has committed to clarify whether cyber risks are covered across property and casualty policies beginning with 2019 renewals (Wood, 2019) and FM Global revised its commercial property policies to address silent cyber from July 2019 (Collins, 2019).*

[68] Lloyd's Market Bulletin Y5258 "Providing clarity for Lloyd's customers on coverage for cyber exposures" and update (Ref. Y527)7

[69] For example, a recent EIOPA survey found that a large share of insurers had not yet begun to address their potential non-affirmative exposure.

[70] University of Cambridge – Centre for Risk Studies and RMS, "Managing Cyber Insurance Accumulation Risk", 2016.

[71] For example, in Lloyd's and University of Cambridge – Centre for Risk Studies, "The insurance implications of a cyber attack on the US power grid", the impact is estimated by applying three scenarios of increasing severity as measured by the days of outage duration and the number of affected generators.

[72] For example in Lloyd's Emerging Risks Report 2017 (in cooperation with Cyence), "Counting the cost, Cyber exposure decoded", loss confidence intervals are estimated by using a stochastic probability loss model which simulates different parameter values for system interruption duration, business dependencies, effectiveness of business continuity contingency planning, etc.

on insureds' vendors, e-commerce revenues, size, industry, expected recovery time, and other data.[73]

Designing scenarios is the most critical aspect of this approach, since it requires some degree of imagination as well as subject matter expertise in order to build highly severe, but still plausible scenarios. In order to provide an appreciable contribution in terms of risk management, scenarios need to be tailored to the specific (re)insurer's portfolio and vulnerabilities; designing scenarios over multiple cyber threats helps (re)insurers to estimate a distribution of potential losses which could inform underwriting as well as reinsurance strategies.

Several studies have been published in this area, which highlight the complexity of scenario analysis and dependence on underlying assumptions.[74]

2.2 Clarity of policies

Based on the literature review, stock-take of supervisory practices and two roundtable sessions with stakeholders, issues concerning the clarity of cyber coverage have been highlighted as a significant concern.

The cyber insurance products offered in the market use different terminology and coverage headings. Some types of losses may be covered in more than one type of policy, either on an affirmative or non-affirmative basis. In addition, some losses are treated differently across jurisdictions due to different legal requirements or public policy frameworks.

These differences create ambiguity/uncertainty on coverage that may create misunderstandings between insurers and policyholders, coverage disputes and potentially unexpected losses for insurers.

2.2.1 *Overlapping coverage*

Coverage for some types of losses from cyber incidents may be available on an affirmative basis in both cyber insurance and other types of policies. For example, losses resulting from social engineering and other types of computer fraud may be covered in a cyber insurance policy and a crime/fidelity policy. Costs related to mitigating or terminating a ransomware attack may be covered in a cyber insurance policy and a kidnap and ransom policy. As a result, policyholders may not be aware of where to seek coverage for these losses or may acquire duplicative coverage.

2.2.2 *Non-Affirmative coverage*

In addition to the exposure measurement challenges identified above, the potential for cyber losses to be covered on a non-affirmative basis in other types of policies creates unhelpful

[73] Lloyd's Emerging Risks Report 2018 (in cooperation with AIR), "Cloud Down, Impacts on the US economy".

[74] For example, in Lloyd's and University of Cambridge – Centre for Risk Studies and , "The insurance implications of a cyber attack on the US power grid", the ineffectiveness of cyber risk exclusionary clauses would cost US insurers USD 5.5 bln more, or 25% under the milder of the standard scenarios analysed.

uncertainty for both insurers and policyholders. Insurers noted that offering cyber coverage only on an affirmative basis should provide more coverage certainty for policyholders.

2.2.3 *Treatment of ransoms, fines, terrorism and war risk*

An example of cyber insurance policy terminology which has been cited as creating uncertainty - and in at least one ongoing instance is the subject of coverage litigation in the United States[75] - is the war exclusion. War exclusions are typically found in cyber risk insurance policies. As the OECD states in its examination of cyber insurance clarity, "coverage for damages and losses from cyber attacks that might be expected to be found in property or liability policies may not materialise if it is determined that the attacks originated from an actor linked to a state or a terrorist organisation."[76]

A great deal of anecdotal literature describes as problematic the potential policyholder uncertainty arising from a war exclusion, particularly in view of the noted "Mondelez" coverage litigation.[77] Others, however, have noted that the war exclusion issue in such case is particularly broad, and that the treatment accorded in such case may, in part, be due to the fact that it arises under a property policy rather than a cyber policy:

"Finally, cyber underwriters understand the risks of cyber attacks better than anyone else in the insurance industry. They are therefore more comfortable covering those risks than a property insurance underwriter might be. As a result, cyber insurers may not feel a need to apply war exclusions to exclude attacks like NotPetya because they understood that risk and intended to cover it."[78]

Similar questions have been voiced with respect to "terrorism" exclusions in the context of cyber insurance. Insurers are much more likely to offer coverage that extends to terrorism – and in some instances may be required to do so.[79] However, distinguishing between and

[75] The litigation, in Illinois state court, is between the insured, Mondelez International, and Zurich American Insurance. It arises under a property policy covering "physical loss or damage to electronic data, programs, or software … caused by malicious introduction of a machine code or instruction," and concerns the 2017 "NotPetya" cyber incident. In the litigation, Mondelez claims that Zurich has denied coverage on the basis of that the damages suffered by its insured arising from the NotPetya malware are subject to an exclusion for loss or damage from a "hostile or warlike action in time of peace or war" by a "government or sovereign power … military, naval, or air force … or agent or authority of" the foregoing. (Case Number 2018-L-011008, Circuit Court Cook County, October 2018)

[76] OECD, "Encouraging Clarity in Cyber Insurance Coverage. The Role of Public Policy and Regulation", 2020.

[77] See, for example, Wall Street Journal " Cyberattacks Complicate War Exclusions for Insurers", (December 6, 2019).

[78] Kevin M. LeCroix, "War Exclusions and Cyber Attacks," The D&O Diary (February 21, 2019), https://www.dandodiary.com/2019/02/articles/cyber-liability/guest-post-war-exclusions-cyber-attacks/.

[79] While it is not mandatory for the policyholder to take up the coverage, pursuant to the Terrorism Risk Insurance Act in the United States, insurers offering insurance in "TRIA eligible" lines are required to make coverage for terrorism available. Guidance issued by the U.S. Treasury Department in 2016 indicates that cyber insurance is generally classified as TRIA eligible, thereby implicating the mandatory offer of coverage. *Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program*, 81 FR 95312 (December 27, 2016), https://www.federalregister.gov/documents/2016/12/27/2016-31244/guidance-concerning-stand-alone-cyber-liability-insurance-policies-under-the-terrorism-risk.

among cyber “terrorism,” cyber “war,” and even cyber “vandalism” will likely continue to present challenges.

In general, most cyber insurance policies with a war exclusion also have a carve-back for cyber terrorism. On the other hand, to the extent that coverage for cyber risks is found in another type of policy, eg property insurance, that carve-back is less likely to be the case.

Some types of losses that may arise as a result of a cyber incident may also be excluded based on public policy or legal considerations. In some countries, insurance coverage for the payment of ransoms is not permitted out of concern that insurance coverage could encourage further extortion. In most cases, these restrictions on insurance coverage were established to address extortion relating to the kidnapping of persons and, therefore, the applicability of this restriction to cyber extortion is not always clear. A further complexity results from the involvement of various sanctioned entities in cyber extortion as insurance reimbursements for payments to sanctioned entities is normally considered a sanctions violation. The fines and penalties imposed as a result of the violation of cybersecurity or privacy requirements, depending on the nature of the fine/penalty, are also uninsurable in some jurisdictions.

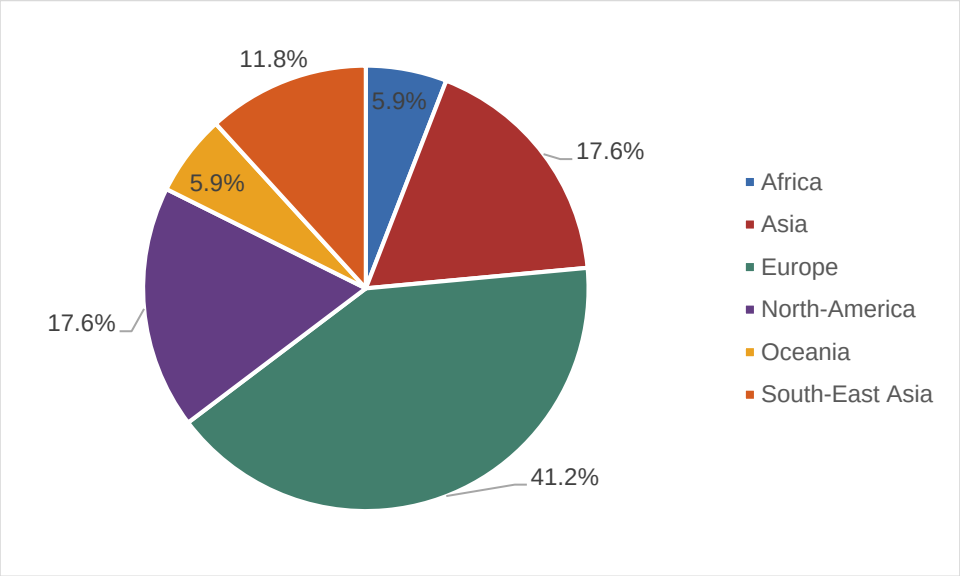
As a result of these questions of legal insurability, most cyber insurance policies impose a condition on coverage for ransoms, fines and penalties based on whether that coverage is permitted by law. A recent OECD analysis[80] found a high-level of uncertainty among insurers regarding the legality of insurance reimbursements for ransom payments and administrative/civil fines and penalties (in some jurisdictions) as well as the responsibilities of insurers for ensuring that reimbursements are not made for payments to sanctioned entities.

3 Regulatory and Supervisory developments

In the last quarter of 2019, the IAIS conducted a stock-take of supervisory practices regarding cyber risk underwriting (the “stock-take”) to collect information on established and/or planned supervisory practices and initiatives regarding cyber risk underwriting among a representative group of IAIS Members. Information was provided by seventeen Members distributed all over the world regions.

[80] OECD (2020), *Encouraging Clarity in Cyber Insurance Coverage. The Role of Public Policy and Regulation*.

Figure 4: Distribution of responding supervisors by Region



The stock-take covered the following topics:

- Monitoring of cyber risk underwriting;
- Supervisory framework and guidance on cyber risk underwriting; and
- Supervisory capacity for monitoring cyber risk underwriting.

3.1 Overview of responses and main findings

Supervisors showed general awareness of the potential challenges associated with cyber-risk underwriting resulting from the development of the cyber insurance market, although at the time of the survey the responding supervisors had not yet developed or implemented specific supervisory practices targeting cyber risk underwriting.

However, most supervisory authorities had launched ad-hoc data collections on cyber risk underwriting in order to better understand the cyber insurance market and insurers' risk management practices for addressing both affirmative and/or non-affirmative cyber risk.

The most common concerns revealed by the stock-take include:

- Risk assessment of cyber risks without sufficient historical loss of data for the assessment;
- Identification and mitigation of non-affirmative cyber risks; and
- Application of the supervisory framework to accommodate additional attention to cyber risk underwriting, such as updating supervisory reporting requirements.

3.1.1 *Monitoring cyber risk underwriting*

The majority of supervisors responded that they had launched, or that they were planning to launch, ad-hoc data collection on cyber risk to understand the cyber market and risk exposures of insurers. Generally, these initiatives targeted the major insurance sector players active in the cyber insurance market, with a focus on affirmative and non-affirmative cyber coverage.

However, very few supervisors require mandatory reporting on cyber risk by insurers. Through the ad-hoc data collection, the majority of supervisory authorities collect aggregate quantitative data (premium, claims payment) on affirmative and non-affirmative cyber risk. In some cases, such a reporting is more detailed and includes the number of policies underwritten and whether cyber coverage is part of packaged policies. Other supervisors collected information on type of cyber products offered and on the significance of non-affirmative cyber coverage.

None of the respondents has introduced mandatory reporting of individual cyber risk-related claims yet. Among ongoing initiatives, EIOPA published a proposal for including cyber risk underwriting in supervisory reporting.[81]

Box 5: NAIC Data Collection

Cybersecurity continues to be important for businesses in the United States to operate effectively and efficiently. In response to the increasing amount of malicious cyber activity, the National Association of Insurance Commissioners (NAIC) was prompted to begin collecting cyber insurance data.

The NAIC began collecting data regarding cyber insurance in 2015 for the 2014 data year. Prior to the NAIC's data collection, there was no clear indication of the size of the cyber insurance market, as the only data collected was via voluntary surveys performed by various organisations.

Prior to the NAIC's Cybersecurity Insurance Supplement in the Property and Casualty Annual Statement, data regarding cyber insurance was collected under the "other liability" section of the state page of the annual statement (ie there was no breakout for cyber insurance under this line item). State insurance regulators believed it was important to begin collecting data on this nascent market to gain an understanding of the cyber insurance market in the United States. Accordingly, the supplement was designed and implemented.

Data elements collected in the NAIC Cybersecurity Insurance Supplement include: (1) the number of claims reported (first-party and third party); (2) direct premiums written and earned; (3) direct losses paid and incurred; (4) adjustment and other expenses paid and incurred; (5) defence and cost containment expenses paid and incurred; and (6) number of policies in-force. If an insurer does not have a breakout available for premium that is part of a package policy, the supplement asks insurers to provide reasonable estimates.

Information is collected from insurers in the admitted market that are required to file the NAIC Property and Casualty Annual Statement. Beginning in 2016, for the 2015 data year, the NAIC collected information from surplus lines carriers. Surplus lines data is not as detailed, but does include: (1) direct premiums written and earned; (2) direct losses paid and incurred; (3) direct adjusting and other expenses; (4) defence and cost containment expenses paid and incurred; (5) number of policies in force; and (6) number of claims reported.

[81] Consultation Paper on proposals for Solvency II 2020 Review; Package on Supervisory Reporting and Public Disclosure (https://www.eiopa.europa.eu/sites/default/files/publications/consultations/eiopa-bos-19-305_qrt_review.pdf).

3.1.2 *Supervisory framework on cyber risk underwriting*

Given the small size of the cyber insurance market, the majority of supervisors have not yet developed specific supervisory frameworks on cyber risk underwriting.

Among respondents, only one supervisor indicated that it has issued a specific statement to clarify its expectation regarding the prudent management of cyber insurance underwriting risk.[82]

Generally, respondents consider existing risk management guidelines and recommendations as broad enough to cover cyber underwriting among the emerging risks. The development of a dedicated supervisory framework will be considered once market volumes achieve a larger scale, and subject to further analysis to identify and document the issues relevant to cyber risk underwriting. Among others, EIOPA has recently defined a strategy to develop specific priorities for cyber risk underwriting in its member jurisdictions.[83]

In light of increasing concerns, however, a certain number of supervisors indicated that they organised awareness-raising events and engaged with the insurance sector in various occasions to discuss on the challenges posed by cyber risk underwriting, particularly by non-affirmative cyber exposure. One supervisor specifically requires insurers to include non-affirmative cyber coverage in their ORSA.

3.1.2.1 Capital requirements

Consistent with the lack of specific supervisory guidelines on cyber risk underwriting, all the respondents indicated that their existing statutory accounting and capital standards do not provide specific treatment for cyber underwriting risk (whether on affirmative or non-affirmative basis). Given the lack of data and the small scale of the market, the majority of respondents do not currently have plans to introduce such requirements in the near future either. Two supervisors, however, will consider including cyber risk policies under catastrophic risk categories.

Various supervisors noted that any significant cyber risk exposure, including any accumulation risk, should be identified and assessed through insurers' stress test based on ORSA, and that in such cases insurers would have to allocate internal capital to cyber underwriting risk. The survey has revealed some ongoing initiatives to develop guidance on accumulation risk from cyber underwriting.

3.1.2.2 Other supervisory areas

A common terminology and or taxonomy is a basis for supervisory activities and communication with insurers and, there is much more work to develop a cross-sectoral taxonomy. Supervisors generally recognise its potential importance for supervisory guidance and reporting, as well as for risk management. The survey has indicated that supervisors consider the development of an international taxonomy as more valuable than national or sectoral ones; to this end, they have signaled their involvement in comprehensive work initiated by international organisations and/or their government (eg the FSB Cyber Lexicon), but no specific terminology/taxonomy for insurance cyber underwriting has been defined yet.

[82] Bank of England, Prudential Regulation Authority "Cyber insurance underwriting risk", Supervisory Statement SS4/17

[83] EIOPA, "EIOPA strategy on cyber underwriting", February 2020, https://www.eiopa.europa.eu/content/cyber-underwriting-strategy_en

Some supervisors have also noted that they are looking at initiatives promoted by the private sector aimed to define taxonomies for cyber incidents and harmonised terminology.

Despite the concerns on non-affirmative coverage and lack of harmonised terminology and or taxonomy, the majority of authorities have not had evidences of significant conduct-related problems or claims/disputes/litigation related to cyber insurance, except for few high-profile cases. This could be in part due to the fact that the cyber insurance market is still an emerging market; however, supervisors will be vigilant on the emergence of any misconduct and will apply existing conduct regulation for cyber insurance.

Finally, the survey indicated that in the majority of respondents' jurisdictions there have not been established government loss-sharing mechanisms for cyber risk. Some respondents noted that existing policyholder protection and terrorism risk insurance schemes could also work for cyber insurance claims, although exclusions exist.[84]

3.1.3 *Supervisory capacity for monitoring cyber risk underwriting*

Supervision of insurance underwriting risk is a new challenge for supervisors. The majority of supervisors consider that they have the necessary resources to monitor and assess the cyber insurance market and the soundness of cyber underwriting risk management by insurers.

However, in light of its current market scale, few respondents indicated that they have included cyber risk underwriting in their supervisory programs. In some cases, supervisors indicated that they are in the process of expanding the number of resources skilled in technological and cyber risks.

3.1.4 *Supervisory concern on cyber risk underwriting*

The main concerns and challenges that supervisors identified with respect to cyber risk underwriting are:

- collecting sufficient cyber incident data to quantify cyber insurance risk and define the appropriate premium rate and risk management approach. Supervisors have concerns about how insurers assess cyber risk in their underwriting processes and manage the underwritten risk;
- identifying and managing non-affirmative cyber risk. Supervisors have concerns that insurers are not fully aware of the extent of their potential exposure to non-affirmative cyber risk in insurance policies. Thus, the identification and measurement of non-affirmative risk remains to be further developed in terms of data adequacy and underwriting standards; and,
- understanding cyber risk accumulations, as cyber risk could entail important systemic risks and uncertainties.

[84] The OECD recently completed an assessment of the coverage provided by terrorism (re)insurance programmes for cyber-terrorism: OECD (2020), *Insurance Coverage for Cyber Terrorism in Australia*, OECD and ARPC.

4 References

Accenture and Ponemon Institute. (2019). *Cost Of Cyber Crime Study.*

Accenture and Ponemon Institute. (2019). *Ninth Annual Cost of Cybercrime Study.* Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Allianz. (2019). *Risk Barometer 2019.*

Allianz. (2019). *RIsk Barometer 2019.*

AM Best. (2019). *Cyber Insurers are profitable today, but wary of tomorrow's risks.*

AM Best. (2019). *Cyber Insurers are Profitable Today, but wary of Tomorrow's Risks .* Retrieved from http://www3.ambest.com/bestweekpdfs/sr507453119175full.pdf

AON. (2017). *2017 Global Cyber Market Overview.*

Aon. (2017). *Cyber Insurance Market Update.* Aon (Australia). Retrieved 02 01, 2019, from http://www.aon.com.au/australia/insights/insurance-market-updates/2017/files/cyber-insurance-market-updates-brochure.pdf

AON. (2019). *Cyber Insurance Market Insights.* Retrieved from https://aoninsights.com.au/cyber-insurance-market-insights-q4-2019/

Bank of England, Prudential Regulation Authority . (2017). *Cyber insurance underwriting risk, Supervisory Statement SS4/17.*

Bank of England, Prudential Regulation Authority. (2019). *Cyber Underwriting Risk Follow-Up: Survey Results .*

Biener C., Eling M. and Wirfs J. H. (2015). *Insurability of Cyber Risk: An Empirical Analysis.* The Institue of Insurance Economics at the University of St. Gallen.

Biener, Eling, Wirfs. (2015). Insurability of cyber risk: an empirical analysis. *University of St. Gallen*.

Cambridge University Center for Risk Studies. (2019). *Cyber Risk Outlook.*

Carrier Management. (2019). AIG Will Finalize Transition to Affirmative Cyber Coverage in January 2020. *Carrier Management*. Retrieved 10 22, 2019, from https://www.carriermanagement.com/news/2019/09/06/197494.htm

Check Point. (2019). *Cloud Security Report: Cloud Security Challenges, Solutions, and Trends.*

Collins, S. (2019). FM Global to charge for data cover and clarify cyber wordings. *Commercial Risk*. Retrieved 10 22, 2019, from https://www.commercialriskonline.com/fm-global-charge-cyber-data-cover-clarify-wordings/

CRO forum. (2015). Casualty Accumulation Risk.

CRO Forum. (2018). *Supporting on-going capture and sharing of digital event data .*

CSIS and McAfee. (2018). *Economic Impact of Cybercrime— No Slowing Down.*

Curti F., Gerlach J., Kazinnik S., Lee M. and Mihov A. (2019). *Cyber Risk Definition and Classification for Financial Risk Management.* Federal Reserve Bank of Richmond.

Deloitte Center for Financial Services. (2018). *2019 Insurance Outlook: Growing economy bolsters insurers, but longer-term trends may require transformation.* Deloitte. Retrieved 01 16, 2019, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-dcfs-2019-insurance-industry-outlook.pdf

Deloitte University Press. (2017). *Demystifying cyber insurance coverage.*

EIOPA. (2018). *Understanding Cyber Insurance – A structured dialogue with insurance companies.*

EIOPA. (2019). *Cyber Risk for Insurers: Challenges and Opportunities.* Retrieved from https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf

EIOPA. (2020). *EIOPA strategy on cyber underwriting .* Retrieved from https://www.eiopa.europa.eu/content/cyber-underwriting-strategy_en

Faulkner, M. (2019). Lloyd's moves to rein in 'silent' cyber exposures. *Insurance Day*. Retrieved 10 22, 2019, from https://insuranceday.maritimeintelligence.informa.com/ID1127905/Lloyds-moves-to-rein-in-silent-cyber-exposures

Federation of European Risk Management Associations (FERMA). (2018). *Preparing for Cyber Insurance.*

Ferland, J. (2019). *Cyber insurance – What coverage in case of an alleged act of war? Based on Mondelez vs Zurich.*

Financial Stability Board (FSB). (2018). *Cyber Lexicon.*

Financial Stability Board (FSB). (2019). *Third-party dependencies in cloud services.*

Franke, U. (2017). The cyber insurance market in Sweden . *Science Direct*.

GFIA . (2018). *GFIA Observations on Cybersecurity.*

Guy Carpenter and CyberCube. (2019). *Looking Beyond the clouds.*

Hiscox . (2018). *Hiscox Cyber Readiness Report 2018 .* Retrieved from https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

Hiscox. (2017). *Hiscox Cyber Readiness Report 2017.* Hiscox. Retrieved 03 26, 2019, from https://www.hiscox.com/documents/brokers/cyber-readiness-report.pdf

Hiscox. (2018). *Hiscox Cyber Readiness Report 2018.* Hiscox. Retrieved 02 01, 2019, from https://www.hiscox.co.uk/sites/uk/files/documents/2018-02/Hiscox_Cyber_Readiness_Report_2018_FINAL.PDF

Hiscox. (2019). *Hiscox Cyber Readiness Report 2019 .* Retrieved from https://www.hiscox.com/sites/default/files/content/documents/2019-Hiscox-Cyber-Readiness-Report.pdf

Howard, L. (2019). Reinsurers Look at Cyber's Massive Growth Possibilities—With Caution. *Carrier Management*. Retrieved 10 24, 2019, from https://www.carriermanagement.com/features/2019/10/18/199207.htm

Hunton & Williams. (2017). *Digital Due Diligence: Four Questions to Evaluate Cyber Insurance Coverage.*

IBM Security and Ponemon Institute . (2019). *Cost of a Data Breach Report: 2019.* Retrieved from https://www.ibm.com/security/data-breach

Institute of International Finance (IIF). (2017). *A growth market adapting to increased demand.*

Institute of International Finance (IIF). (2019). *Cyber Risk Insurance Update: Advances in Risk Management, Prioritisation, Prevention and Protection.*

Institute of International Finance. (2018). *Addressing regulatory fragmentation to support a cyber resilient global financial services.*

Johansmeyer, T. (n.d.). Short-Term, Short-Tail. *the OECD Conference on Unleashing the Potential of the Cyber Insurance Market (22-23 February 2015, Paris), https://www.oecd.org/daf/fin/insurance/Presentations-Conference-cyber-insurance-market.pdf*, (p. 2018).

LeCroix, K. M. (2019). *War Exclusions and Cyber Attacks The D&O Diary .* Retrieved from The D&O Diary : https://www.dandodiary.com/2019/02/articles/cyber-liability/guest-post-war-exclusions-cyber-attacks/

Lloyd's. (2019). *Market Bulletin Y5258 "Providing clarity for Lloyd's customers on coverage for cyber exposures" and update (Ref. Y527).*

Lloyd's and University of Cambridge – Centre for Risk Studies. (2015). *The insurance implications of a cyber attack on the US power grid.*

Lloyd's Emerging Risks Report 2017 (in cooperation with Cyence). (2017). *Counting the cost, Cyber exposure decoded.*

Lloyd's Emerging Risks Report 2018 (in cooperation with AIR). (2018). *Cloud Down, Impacts on the US economy.*

Looyd's and Cambridge University Centre for Risk Studies. (2015). *Emerging Risks Report – 2015 Business Blackout.*

Lubin, A. (2018). *Insurability of Cyber Risk.*

Marsh. (2020). *COVID-19: Cybersecurity Checklist for Remote Working".* Retrieved from https://coronavirus.marsh.com/us/en/insights/research-and-briefings/covid-19-cybersecurity-remote-working.html

Marsh, Marsh & McLennan Companies. (2019). *2018 Cyber Insurance Trends: Purchasing, Limits and Pricing .* Retrieved from https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/cyber-insurance-trends-report-2018.pdf

Munich Re. (2018). *Cyber insurance market outlook*. Retrieved from , https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-market-outlook-2018.html

National Association of Insurance Commissioners (NAIC). (2019). *Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement .* Retrieved from https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final%20%281%29.pdf.

NetDiligence. (2019). *Cyber Claims Study .*

OECD. (2017). *Enhancing the Role of Insurance in Cyber Risk Management.* OECD. Retrieved 05 28, 2018, from http://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf

OECD. (2020). *Encouraging Clarity in Cyber Insurance Coverage. The Role of Public Policy and Regulation.*

OECD. (2020). *The role of public policy and regulation in enhancing the availability of data for cyber insurance underwriting.*

OECD and ARPC. (2020). *Insurance Coverage for Cyber Terrorism in Australia.*

Orbis Research. (2018). *Global Cyber Security Insurance Market 2018.* Retrieved 01 16, 2019, from https://www.reuters.com/brandfeatures/venture-capital/article?id=36676

Partner Re and Advisen. (2019). *Cyber Insurance: The Market's View, Partner Re and Advisen .* Retrieved from https://partnerre.com/wp-content/uploads/2019/10/Cyber_Insurance_The_Markets_View_2019-1.pdf.

Romanosky S. et al. (2018). *Content analysis of cyber insurance policies: how do carriers price cyber risk?* Journal of Cybersecurity.

SANS Institute. (2016). *Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey.*

Swiss Re . (2017). Cyber risks in an interconnected world.

Swiss Re . (2019). *Could cyber risk be a growth engine for reinsurance? .* Retrieved from https://www.swissre.com/reinsurance/property-and-casualty/reinsurance/cyber-reinsurance/reinsurance-a-growth-engine-for-cyber.html

Swiss Re Institute. (2017). *Cyber: getting to grips with a complex risk.*

The Council of Insurance Agents and Brokers (CIAB). (2019). *Cyber Insurance Market Watch Survey: Executive Summary (Fall 2018) .* Retrieved from https://www.ciab.com/download/16876

The Geneva Association. (2018). *Advancing Accumulation Risk Management in Cyber Insurance.*

The Geneva Association. (2018). *Contours of an emerging market for cyber risk transfer.*

The Geneva Association. (2018). *Cyber Insurance as a Risk Mitigation Strategy.*

The Geneva Association. (2018). *Ten Key Questions on Cyber Risk and Cyber Risk Insurance.*

University of Cambridge – Centre for Risk Studies and RMS. (2016). *Managing Cyber Insurance Accumulation Risk.*

US Department of Treasury. (2016). *Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program, 81 FR 95312.* Retrieved from https://www.federalregister.gov/documents/2016/12/27/2016-31244/guidance-concerning-stand-alone-cyber-liability-insurance-policies-under-the-terrorism-risk

Wall Street Journal. (2019). *Cyberattacks Complicate War Exclusions for Insurers.*

Wood, C. (2019). *Allianz to address silent cyber with updated policy wordings.* Retrieved 10 24, 2019, from https://www.reinsurancene.ws/allianz-to-address-silent-cyber-with-updated-policy-wordings/