Enhancing the Availability of Data for Cyber Insurance Underwriting

THE ROLE OF PUBLIC POLICY AND REGULATION

Please cite this publication as:

OECD (2020), *Enhancing the Availability of Data for Cyber Insurance Underwriting, The Role of Public Policy and Regulation.* www.oecd.org/finance/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.pdf

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Foreword

The increased reliance on digital technologies has led to increasing digital security and privacy risks and the emergence of a cyber insurance market to provide policyholders with financial protection against many of those risks. The stand-alone cyber insurance market has grown rapidly in recent years and surveys have found an increase in take-up among both large and small businesses. However, despite the growth in premium volume and take-up, the affirmative cyber insurance market remains small relative to other commercial insurance business lines.

In 2018, the OECD organised a Conference on Unleashing the potential of the cyber insurance market[1] with a view to building some consensus around how different stakeholders could contribute to addressing the main challenges to the market's development. The inability to adequately quantify exposure to cyber risks is commonly understood to be one of the most significant impediments to the development of the cyber insurance market. This limits both insurance buyers' understanding of their insurance needs and insurance companies' willingness to extend significant coverage for cyber risks.

This report examines the impact of legislation, regulation, guidance and other public policy measures (henceforth referred to as "public policy and regulation") on the lack of data on past incidents necessary for underwriting, including the role of governments in facilitating information sharing on cyber threats and incidents and addressing any legal impediments to information sharing. The development of this report has been informed by responses to a questionnaire provided by OECD member and non-member authorities as well as informal consultations with (re)insurance industry representatives undertaken in September and October of 2019. Responses to the questionnaire were received from Argentina, Austria, Belgium, Bermuda, Brazil, Chile, Colombia, Estonia, France, Germany, Italy, Japan, Latvia, Lithuania, Portugal, Russian Federation, Slovak Republic, Slovenia, South Africa, Switzerland, the United Kingdom and the United States.

Encouraging clarity in cyber insurance coverage: The Role of Public Policy and Regulation is a complementary report focusing on ways to address some of the most common policyholder misunderstandings around insurance coverage for cyber risks. *Insurance Coverage for Cyber Terrorism in Australia* assesses the potential gaps in insurance coverage for cyber-terrorism and other politically-motivated and destructive attacks, both in Australia and internationally.

Table of contents

Boxes

1 The implications of public policy and regulation on claims data sharing

Data on past incidents is a critical input across many lines of business for estimating the likely frequency and magnitude of claims and for calibrating the models that are often used for premium pricing and capital allocation. For other perils, underwriting is usually based on actual past losses and claims which allow for estimates of probability and severity – or, for lower frequency risks, dedicated models that estimate loss probability based on the interaction between hazard frequency and magnitude, exposure and vulnerability (often calibrated using data on past losses and claims).

Public policy and regulation could potentially have an impact on the ability of insurance companies to share information on past cyber incidents affecting their policyholders (or, specifically, information on claims). Insurance companies may not be able to share this information as a result of specific insurance legislation. In addition, public policy or regulation in other areas, such as privacy or anti-trust requirements, could constrain the ability of insurance companies to share (some types of) policyholder information or to collaborate with other insurance companies.

However, only two of the countries that responded to the OECD's questionnaire identified a specific public policy or regulatory constraint to the development of a repository or other form of information sharing on past cyber incidents (although a number of others noted the potential for issues to be raised by privacy regulation). In addition, the Federal Ministry of Finance of Austria indicated that data protection requirements as well as practical impediments such as reporting requirements, administrative burden and liability issues would likely impede the ability to develop a cyber incident repository.

Anti-trust considerations

Competition or anti-trust public policy and regulation aims to promote market competition by restraining anti-competitive practices. The sharing of sensitive commercial information among competitors is normally considered to be anti-competitive to the extent that it restricts competition. For example, exchanging information on business objectives or pricing strategies could lead companies to adapt their strategies to account for the practices of competitors (as in a cartel), and therefore distort normal market competition.

Within the insurance sector, information on past claims or claims experience is a critical input to underwriting and pricing which, if shared, could provide competitors with some insight into pricing approaches. However, the aggregation of data on past claims across many companies can also provide efficiency gains as more comprehensive data could support more accurate pricing of risk. As a result, competition policy and regulation in a number of jurisdictions allows (or has allowed) some cooperation among insurance companies in the area of information exchange related to past claims and losses:

- In the European Union, a Communication from the Commission in 2011 provides guidance on the application of competition law to "horizontal co-operation agreements" including agreements that involve information exchange (a specific exemption for such arrangements expired in 2017[2]). The guidelines suggest that information that is aggregated without the ability to decipher the source company and that is historic is less likely to have restrictive effects on competition (European Commission, 2011[1]). A recently announced European Commission investigation into the pooling of motor vehicle claims data in Ireland affirmed that competition authorities in the European Commission recognise the potential for data pooling arrangements to contribute to effective competition (European Commission, 2019[2]).[3]

- In the United States, data pooling arrangements could be considered a violation of anti-trust requirements. However, the McCarran Ferguson Act, which aims to ensure the pre-eminence of state regulation of insurance, provides a limited exemption for insurance companies from Federal anti-trust requirements in areas (such as premium ratings) where states have enacted legislation (Nordman, 2017[3]).[4]

In addition to the potential efficiency gains from information exchange for the pricing of risk, the sharing and aggregation of data on past claims might enhance competition by facilitating market entry by new insurers and supporting a more level playing field between insurers with different levels of claims experience (large vs. small, incumbents vs. new entrants) (Insurance Information Institute, 2019[4]). A number of (re)insurance companies consulted during the development of this report suggested that cyber insurance claims data sharing could support competition in the market as there are a few large providers of cyber insurance who may benefit from a competitive advantage as a result of their significantly greater access to past claims data (which may also be an impediment to data sharing – see below). Some suggested that greater access to claims data through information exchange might also lead to a more sustainable market as new entrants without historical experience would have a firmer basis for underwriting their coverage.

The rationale for allowing cooperation among insurers may be greater for risks that are new or that transpire less frequently (such as cyber risk) where there is more limited experience, higher levels of uncertainty or other challenges to the insurability of those risks. Insurance associations (e.g. Insurance Council of Australia) and private sector entities (e.g. Insurance Services Office and Property Claims Service, Perils) collect and publish aggregate insured loss data for significant catastrophe events. In France and Norway, insurance companies share geo-coded claims data related to natural catastrophe losses (see Box 1.1). In Germany, the German Insurance Association (GDV) collects a range of statistics, including for loss experience. GDV member companies provide this data on a voluntary basis and the results are available to those that contribute data.

Box 1.1. Sharing of catastrophe claims data (France and Norway)

In France and Norway, the insurance associations play a role in collecting and aggregating data on catastrophe claims in order to support the availability of information on disaster risks. In Norway, the banking and insurance association (*Finans Norge*) collects data on water-related claims at the level of individual addresses and shares that data with municipalities in order to inform investments in disaster risk reduction. In France, the insurance association (*Fédération Française de l'Assurance*) established an organisation (*Mission risques naturels*) to collect and aggregate claims data from natural catastrophes and make risk assessment tools available for insurance companies and the general public through a public-private partnership with the national government (*Observatoire National des Risques Naturels*).

Privacy/confidentiality requirements

The ability of (re)insurance companies to provide claims or other data to a data repository could be impeded by legal requirements imposed under privacy or insurance legislation or regulation or as a result of contractual commitments made to policyholders (or ceding insurers).

Similar to other legal entities, insurance companies must comply with privacy protection regulations related to the collection, use and disclosure of personal information that they collect from entities applying for insurance, acquiring insurance coverage and making claims under their insurance coverage. However, privacy protection requirements, which have been established in most (if not all) OECD countries, are generally targeted at the collection of “personal information”.[5] Generally, the definition of personal information would not apply to information related to the legal persons/corporate entities that are the main acquirers of cyber insurance coverage.

Insurance companies would also need to comply with any specific requirements imposed by insurance regulators or supervisors related to the handling of personal or confidential information. In Portugal, legislation governing insurance contracts imposes a general obligation on insurance companies to maintain the secrecy of all information that is disclosed as part of the execution of the insurance policy. In Latvia, all insurance contract details are required to be kept confidential. In the United States, the National Association of Insurance Commissioners has developed an *Insurance Data Security Model Law* for implementation by state insurance commissions. The Model Law requires insurance companies to maintain the confidentiality of “nonpublic information” which includes both personal information[6] as well as business information of an insurance company or intermediary that, if disclosed, would cause a material adverse impact to its business. The business information of a corporate policyholder does not appear to be captured within the scope of nonpublic information to which the confidentiality requirements apply.

In addition to complying with regulatory requirements established by privacy or insurance authorities, (re)insurance companies may enter into a contractual agreement with policyholders (or ceding insurers) to maintain the confidentiality of the information they collect, including any information on claims (for example, through non-disclosure agreements that may be established in the aftermath of major incidents).

Some insurance companies include a specific statement of their privacy policy or obligations to their policyholder in their policy wordings. For example, many of the cyber insurance policies reviewed for Australian policyholders include a specific statement on privacy commitments in policy documentation, including the types of information that is collected, how it will be used and to whom it may be disclosed[7] (including whether information might be disclosed to an entity in a third country). This practice seems to be less common in other jurisdictions although at least one example was found in a policy offered to European policyholders.

The privacy-related obligations of – and commitments made by - insurance companies are normally applicable to any entity providing “personal information” through their website or more generally. In most cases, a plain-language assessment of the commitments that insurance companies have made to their policyholders seems to preclude the sharing of “personal information” with a third party non-governmental entity mandated to collect and share data on past incidents and claims (with a few exceptions[8]). However, the use of personal information for data analytics is likely only to be necessary (or relevant) in certain lines of personal insurance business (e.g. health, life, motor vehicle, property). It is not clear that personal information would be necessary for the analysis of past cyber incidents and claims affecting legal rather than natural persons (and even if it were, it may be possible to seek permission to share that data for public interest purposes).[9]

That some insurance companies are sharing cyber claims information (in some form) with third parties (such as NetDiligence) – without specifically naming or describing them as entities receiving personal information in privacy policies/statements– suggests that such sharing may not constitute a breach of privacy protection requirements or commitments (otherwise, those insurance companies would be in breach of their regulatory obligation) – either because the information that is being shared is not (protected) personal information or the sharing of that information is allowed. In France, where information on natural catastrophe claims is shared with a dedicated organisation related to the insurance association (see Box 1.1), insurance companies do indicate that personal information may be disclosed to professional organisations (e.g. authorised professional organisations, professional or insurance organisations).[10]

2 Market developments and perspectives

There have been a number of efforts to collect and make available general information on past incidents by both government agencies and commercial firms. Computer security incident response teams, privacy protection authorities and sectoral regulators often publish information on the number and type of incidents that have been reported to them. A variety of commercial research and cyber security firms publish statistics on the occurrence of data breaches, malware infections, denial-of-service attacks and other cyber incidents. Financial institutions also share technical information on operational incidents that they have encountered, including cyber incidents, through dedicated platforms aimed at supporting better management and quantification of operational risks.

There have also been a number of efforts within the insurance sector to make information on past cyber losses and claims available. The CRO Forum, a group of insurance and reinsurance companies, leveraged an industry operational risk platform to undertake a pilot exercise to share anonymised information on incidents affecting member companies based on a shared taxonomy (CRO Forum, 2018[5]). Some insurance companies are providing information on the cyber-related claims that they have incurred, either in their own marketing and educational publications or through companies that consolidate that data. One annual analytical report on claims data (NetDiligence) achieved a 50% increase in the number of insurance industry contributors, a 450% increase in the number of claims analysed and an almost 300% increase in insured loss estimates between 2013 and 2017 (NetDiligence, 2014[6]), (NetDiligence, 2018[7]) – although this likely still only accounts for less than 10% of all cyber-related claims payments. Verisk, in the United States, has also launched an initiative to pool data among willing companies on premiums, insuring agreements and claims (including attack characteristics and losses (Verisk Analytics, n.d.[8]). The Verisk Cyber Data Exchange will provide aggregated data to contributing insurers beginning in the first quarter of 2020 and has reportedly received commitments or expressions of interest from more than 10 providers of cyber insurance. The German Insurance Association is collecting, on a voluntary basis, basic data on premiums, coverage, policyholder sector and losses from insurance companies underwriting cyber insurance. The Ministry of Finance of the Slovak Republic indicated that an insurance claims register focused on motor vehicle claims is also used for claims related to cyber incidents.

There has also been significant improvements in the availability of models for managing cyber risk. The two major commercial catastrophe modelling firms released probabilistic cyber models for use in underwriting in 2018 (AIR Worldwide, 2018[9]), (RMS, 2018[10]). A number of specialised modelling firms have also emerged to provide analytics for underwriting cyber risk (OECD, 2018[11]).

The (re)insurance companies consulted during the development of this study indicated that all of these types of data sources (incident data from external parties, claims data - particularly own data - and models) contribute to underwriting the cyber insurance coverage that they provide. None of these data sources on their own provide sufficient information for underwriting coverage as incident data is seen to be incomplete, historical experience covers too few claims and models are relatively new and untested.

There is general agreement that the lack of data on cyber incidents and claims is a challenge for cyber insurance underwriting and that a repository of incident and claims data that leverages the experience of multiple (re)insurers (potentially from multiple countries) would provide an improved basis for underwriting cyber insurance coverage.

The insurance sector and insurance regulators and supervisors are continuing to work on improving the availability of past cyber claims and incident data. The Geneva Association has been examining data sharing mechanisms and potential options to facilitate or promote an enhancement in the access and quality of data and recently announced that the Cyber Incident Data Exchange and Repository (CIDER) would be implemented by a consortium of insurers and reinsurers (The Geneva Association, 2020[12]). In the United Kingdom, insurers are discussing the possibility of accessing data related to data breach notifications made to the Information Commissioner (ABI, 2019[13]) (although there is some concern about the value of this data as it is self-reported). The Insurance Council of New Zealand has recently recommended the establishment of a register of data breaches (ICNZ, 2019[14]). The European Insurance and Occupational Pensions Authority (EIOPA) recently suggested that a European-wide cyber incident reporting database could support the development of the European cyber insurance market (EIOPA, 2019[15]) (also a recommendation made by the International Underwriting Association in 2018 (IUA, 2018[16])) while international collaboration on improving the availability of cyber incident data has been part of the EU-U.S. Insurance Dialogue Project.[11] In its response to a recommendation on improving the availability of cyber incident data for cyber insurance underwriting, the Bank of England has committed to working with HM Treasury and other authorities to encourage greater cyber-incident data sharing (Bank of England, 2019[17]).

The (re)insurance companies and intermediaries consulted during the development of this report indicated that achieving consistency with anti-trust obligations would be the most challenging public policy issue to address for a data repository. However, it is recognised that there are a number of existing examples and mechanisms that provide an approach to addressing anti-trust concerns (e.g. Insurance Services Office in the United States). These claims sharing examples (including the cyber-specific examples noted above, such as NetDiligence), suggest that the sharing of claims data is not necessarily counter to competition/anti-trust public policy and regulation (or at least that any anti-trust concerns related to information exchange agreements can be overcome).

Privacy protection regulation is not considered to be a significant constraint to sharing information on past cyber claims as most of the data collected during the claims handling process would not be protected personal information referring to a natural person. However, the ability of (re)insurance companies to share information on policyholder incidents and claims could be constrained by non-disclosure commitments that have been made to policyholders (whether the corporate policyholders of direct insurers or cedant policyholders of reinsurers). If the incident or claims data shared by a (re)insurer were to become attributable to a specific policyholder (e.g. through ineffective anonymisation), the (re)insurer that provided that data would likely face a damaged customer relationship if not a financial liability. Companies operating in jurisdictions where there are confidentiality requirements that apply to insurance contracts would also be impeded from sharing data on policyholder incidents and claims.

A more significant impediment could be the willingness of large underwriters to participate in any incident or claims data sharing initiative as the benefits would be greatest for those insurers with more limited claims experience. Many of the largest underwriters of cyber insurance have invested significantly in becoming market leaders and consider their claims experience to be a source of competitive advantage and part of their intellectual property. Among the major underwriters consulted, there were important differences in terms of the willingness to participate voluntarily in an incident or claims data sharing initiative.

3 The potential role of regulators and supervisors

The development of an incident and claims data sharing initiative for cyber risks could address one of the most significant challenges to the development of the cyber insurance market. There do not appear to be significant legal or regulatory impediments to the development of an incident or claims data sharing initiative in most jurisdictions. Anti-trust legislation does not generally preclude the establishment of data sharing arrangements in the insurance sector (although any initiative will need to be carefully designed to ensure compliance with anti-trust law) while the information to be exchanged would normally only involve legal persons not covered by privacy regulations. However, such an arrangement would likely not be possible in jurisdictions that have legal requirements on the confidentiality of information related to insurance contracts. The most significant impediment is likely to be the willingness of (re)insurance companies to participate in an incident and claims data sharing initiative, due to confidentiality commitments made to policyholders (and the potential liability that could result from disclosure), uncertainty about whether the value of data sharing outweighs the costs or a desire to maintain their competitive position.

In many existing cases, claims data sharing initiatives have been led by the industry – and particularly by insurance associations – rather than by regulators or supervisors. These initiatives have generally been established to support better risk management (including underwriting in some cases). Therefore, an approach that widely shares the benefits of incident and claims experience might be more acceptable to all stakeholders involved. For example, corporate policyholders might be willing to allow disclosure to a repository of the incidents that have affected them if useful cybersecurity lessons can be derived (and shared) as a result or if the greater availability of data would lead to reduced uncertainty in premium-setting and a consequent reduction in premiums. In addition, the large underwriters may see more benefit in contributing to a repository that ultimately supports greater cyber resilience of policyholders (or avoids less responsible underwriting practices in the market).

Regulators and supervisors will need to carefully consider whether there is a public policy rationale for requiring the (re)insurance companies that they oversee to participate in any incident or claims data sharing initiative (whether established at the national or international level):

Such an initiative could conceivably improve the contestability of the cyber insurance market by providing smaller companies and new entrants with an improved basis for underwriting coverage. However, in many countries, the cyber insurance market is already highly-competitive with many entrants. For example, in the United States, the number of insurance companies underwriting cyber insurance increased from 471 in 2017 to 528 in 2018 (Insurance Journal, 2019[18]).

Access to a larger incident and claims dataset could also potentially improve the quality of underwriting, particularly among underwriters with more limited historical experience. If there are regulatory or supervisory concerns about the quality of cyber insurance underwriting, regulators or supervisors could consider compelling participation in an incident and claims data repository. In a competitive market, all (re)insurance companies should benefit from sound underwriting across the market.

However, any regulatory or supervisory effort to support the establishment and operation of an incident and claims data repository would also need to consider whether the repository would sufficiently improve underwriting quality in the context of a risk that is constantly evolving. Some of the (re)insurance companies consulted questioned the value of a repository given the changing nature of the threat and security environment – although others suggested that aggregated today would facilitate a quicker identification of loss trends.

Box 3.1. Enhancing the availability of data for cyber insurance underwriting: recommendations

- Insurance regulators and supervisors should remove any insurance legislation or regulation that impedes the sharing of data on cyber insurance incidents and claims (e.g. confidentiality requirements applied to information related to insurance contracts).
- Given the potential reluctance of some (re)insurers to be involved in voluntary data sharing initiatives, governments should consider encouraging industry associations (insurance associations and risk management associations) to establish mechanisms for the sharing of incident and claims data and emphasise the critical contribution of better data to supporting risk management, sound underwriting and a competitive market for cyber insurance.
- International collaboration would support the development of a broader and deeper dataset and enhance the benefits of data sharing. Therefore, it will be critical for governments to encourage coordination among national insurance and risk management associations.

References

ABI (2019), *Cyber insurance payout rates at 99%, but uptake still far too low*, Association of British Insurers (web page), https://www.abi.org.uk/news/news-articles/2019/08/cyber-insurance-payout-rates-at-99-but-uptake-still-far-too-low/. [13]

AIR Worldwide (2018), *AIR Develops Advanced Probabilistic Model for Global Cyber Risks*, https://www.air-worldwide.com/Press-Releases/AIR-Develops-Advanced-Probabilistic-Model-for-Global-Cyber-Risks/. [9]

Bank of England (2019), *The future of finance: Summary table of our response*, https://www.bankofengland.co.uk/-/media/boe/files/report/2019/response-to-the-future-of-finance-report-summary-table.pdf?la=en&hash=B89195D26E9932F818F2CFDB76B31102893A8A45. [17]

CRO Forum (2018), *Supporting on-going capture and sharing of digital event data*, www.thecroforum.org/wp-content/uploads/2018/02/201802_CROF_Capture_and_sharing_of_digital_event_data.pdf. [5]

Deloitte Center for Financial Services (2018), *2019 Insurance Outlook: Growing economy bolsters insurers, but longer-term trends may require transformation*, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-dcfs-2019-insurance-industry-outlook.pdf. [19]

EIOPA (2019), *Cyber Risk for Insurers – Challenges and Opportunities*, European Insurance and Occupational Pensions Authority, https://eiopa.europa.eu/Publications/Reports/EIOPA_Cyber%20risk%20for%20insurers_Sept2019.pdf. [15]

European Commission (2019), *Commission opens investigation into Insurance Ireland data pooling system*, European Commission Press Release, https://europa.eu/rapid/press-release_IP-19-2509_en.htm. [2]

European Commission (2011), *Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements (Communication from the Commission)*, Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011XC0114(04)&from=EN. [1]

European Union (2016), *Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. [25]

EU-US Insurance Dialogue Project Steering Committee (2018), *EU-US Insurance Dialogue Project: New Initiatives for 2017 – 2019: Focus Areas for 2018*, EU-US Insurance Dialogue Project, https://www.treasury.gov/initiatives/fio/EU-US%20Insurance%20Project/Documents/EU-US_Initiatives_2017-2019.pdf. [28]

Howard, L. (2019), “Reinsurers Look at Cyber’s Massive Growth Possibilities—With Caution”, *Carrier Management*, https://www.carriermanagement.com/features/2019/10/18/199207.htm. [22]

ICNZ (2019), *Policies for a Responsive and Sustainable Insurance Sector to Safeguard New Zealand*, Insurance Council of New Zealand, https://www.icnz.org.nz/fileadmin/Assets/PDFs/Publications/Supporting_document_for_ICNZ_Infographic_-_October_2019.pdf. [14]

Insurance Information Institute (2019), *Antitrust Law and Insurance*, Insurance Information Institute, https://www.iii.org/article/antitrust-law-and-insurance. [4]

Insurance Journal (2019), "State of the Cyber Insurance Market— Top Trends, Insurers and Challenges: A.M. Best", *Insurance Journal*, www.insurancejournal.com/news/national/2019/06/18/529747.htm. [18]

IUA (2018), *IUA cyber group calls for registry of claims data*, International Underwriting Association, https://www.iua.co.uk/IUA_Member/Press/Press_Releases_2018/IUA_cyber_group_calls_for_registry_of_claims_data.aspx. [16]

Lloyd's Market Association (2017), *Competition Law Guidance (Updated March 2017)*, https://www.lmalloyds.com/lma/readfile.aspx?iDocumentStorageKey=4fb87012-d6d4-40ec-a752-f05766bd40dd&iFileTypeCode=PDF&iFileName=Competition_Law_Guidance. [23]

NAIC (2017), *Insurance Data Security Model Law*, National Association of Insurance Commissioners, https://www.naic.org/store/free/MDL-668.pdf. [27]

NetDiligence (2018), *Cyber Claims Study 2018*, https://netdiligence.com/wp-content/uploads/2018/11/2018-NetDiligence-Claims-Study_Version-1.0.pdf. [7]

NetDiligence (2014), *Cyber Claims Study 2014*, https://netdiligence.com/wp-content/uploads/2017/03/NetDiligence_2014-Cyber-Claims-Study.pdf. [6]

Nordman, E. (2017), *The relevance of the McCarran-Ferguson Act*, National Association of Insurance Commissioners, http://www.naic.org/cipr_newsletter_archive/vol22_mccarran-ferguson.pdf. [3]

OECD (2018), *Unleashing the Potential of the Cyber Insurance Market: Conference Outcomes*, http://www.oecd.org/daf/fin/insurance/Unleashing-Potential-Cyber-Insurance-Market-Summary.pdf. [11]

OECD (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, http://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf. [21]

OECD (2013), *The OECD Privacy Framework*, www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [26]

Orbis Research (2018), *Global Cyber Security Insurance Market 2018*, https://www.reuters.com/brandfeatures/venture-capital/article?id=36676. [20]

RMS (2018), *RMS Releases Industry's First Probabilistic Cyber Risk Model*, RMS, https://www.rms.com/newsroom/press-releases/press-detail/2018-03-07/rms-releases-industrys-first-probabilistic-cyber-risk-model. [10]

The Geneva Association (2020), *Exploring the opportunity for a Cyber Incident Data Exchange and Repository (CIDER)*, The Geneva Association: News, https://www.genevaassociation.org/news/articles-interest/exploring-opportunity-cyber-incident-data-exchange-and-repository-cider. [12]

United States Congress (115th, 1. (2017), *An Act to restore the application of the Federal antitrust laws to the business of health insurance to protect competition and consumers (in the US Senate)*, https://www.congress.gov/115/bills/hr372/BILLS-115hr372rfs.pdf. [24]

Verisk Analytics (n.d.), *Verisk's Cyber Data Exchange*, Verisk, https://www.verisk.com/insurance/products/cyber-data-exchange/. [8]

Notes

[1] www.oecd.org/finance/insurance/2018-oecd-conference-cyber-insurance-market.htm.

[2] The Insurance Block Exemption Regulation (IBER) provided an exception to competition law requirements for arrangements for the sharing and/or aggregation of data in statistics and studies and for the operation of co-insurance pools aimed at sharing certain types of risks. The IBER protections were not renewed at their expiry in March 2017 (Lloyd's Market Association, 2017[23]).

[3] The Commission's investigation in this case is focused on whether the conditions placed on access to the data pool may have placed companies without access at a competitive disadvantage (European Commission, 2019[2]).

[4] Proposed federal legislation to eliminate the general exemption from federal anti-trust laws for health insurance providers makes an exception to allow for arrangements to "collect, compile, or disseminate historical loss data" to be maintained, suggesting that the pooling of loss data may not be perceived as a significant impediment to competitive markets (United States Congress (115th, 2017[24]).

[5] The regulatory definition of "personal information" varies across jurisdictions although jurisdictions often apply two tests for defining whether information is personal information: (i) that the information relates to an identifiable (natural) person; and (ii) that the information allows for the identification of that individual. In the European Union, for example, personal data means "any information relating to an identified or identifiable natural person who can be identified directly or indirectly with that information" (European Union, 2016[25]) The Recommendation of the OECD Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013 defines personal data as "any information relating to an identified or identifiable individual (data subject)" (OECD, 2013[26]).

[6] The Model Law specifically refers to "information concerning a Consumer" and that can be used to identify a Consumer where a "Consumer" refers to an individual resident of the given state (NAIC, 2017[27]).

[7]The lists of entities to which personal information may be disclosed generally include entities that are part of the same corporate group as the insurer, business partners, other insurers, reinsurers and intermediaries involved in the provision of coverage, various types of service providers and government and regulatory authorities. Most lists of service providers include entities such as IT services and marketing providers, contractors related to loss adjustment, accountants, lawyers, actuaries and banks and other financial institutions. A few privacy policies also indicate that personal information could be shared with organisations involved in fraud detection.

[8] In one policy offered in Europe, the list of entities to whom personal information may be disclosed includes research and survey organisations. In Australia, two policies list the possibility of disclosing personal information to third party providers of data analytics functions.

[9] For example, we understand from *Finans Norge*, the organisation that collects and aggregates the catastrophe claims data (including addresses, which are considered personal information), that permission was sought from the data protection authority to share this information for a public interest purpose.

[10] In Norway, only one privacy policy was reviewed as other companies only provided their policies in Norwegian. The privacy policy reviewed indicates the possibility of disclosing personal information to specific joint registers related to health and life insurance through the insurance association although a specific mention of the catastrophe claim information sharing arrangement was not found.

[11] The EU-U.S. Insurance Dialogue Project Steering Committee identified Cybersecurity Risk and Cyber Insurance Market as one three areas for continued work from 2018 (EU-US Insurance Dialogue Project Steering Committee, 2018[28]). In its response to the OECD questionnaire, the National Association of Insurance Commissioners and the Federal Insurance Office indicated that information sharing on past cyber incidents is one of the project work streams.

www.oecd.org/finance/insurance