31 October 2018

EU-U.S. INSURANCE DIALOGUE PROJECT

THE CYBER INSURANCE MARKET

The EU-U.S. Insurance Dialogue Project (EU-U.S. Project) began in early 2012, as an initiative by the European Commission, the European Insurance and Occupational Pensions Authority (EIOPA), the Federal Insurance Office of the U.S. Department of Treasury (FIO), and the National Association of Insurance Commissioners (NAIC) to enhance mutual understanding and cooperation between the European Union (EU) and the United States for the benefit of insurance consumers, business opportunity, and effective supervision. In 2018, the EU-U.S. Project's members continued the work focusing on the cyber insurance market besides the other focus areas relating to cybersecurity risk, the use of big data and intra-group transactions.[1]

I. Introduction

Recognizing that cyber risk is growing and evolving, both for the insurance sector itself and for those whom it serves, the EU-U.S. Insurance Project is pursuing a bilateral dialogue to share information with respect to this dynamic area of the insurance sector.[2] In order to advance the dialogue, this paper outlines developments in the cyber insurance market, including steps insurers, policymakers, and insurance regulators are taking to ensure that such products are being offered in a sound and prudent manner.[3] The paper first describes the cyber insurance market, and the types of available cyber insurance coverage. Next, the paper outlines challenges in underwriting cyber insurance. It then highlights current supervisory practices for assessing cyber insurance underwriting. The paper concludes by offering proposals for future dialogue by Project members.

II. Cyber insurance market and coverage types

Although the first cyber insurance policy was written more than twenty years ago, cyber insurance products are a relatively new addition to the property & casualty (P&C) market.[4] Definitions vary, but generally cyber insurance may be understood as products covering losses arising from malicious and non-malicious incidents relating to the handling, storage, and transmission of electronic data, including through the Internet and computer networks.[5] Cyber insurance products may offer coverage for various

---

[1] New initiatives for 2017 – 2019 including focus areas for 2018: https://eiopa.europa.eu/external-relations/regulatory-dialogues

[2] *EU-US Insurance Dialogue Project: New Initiatives for 2017-2019*, https://www.treasury.gov/initiatives/fio/EU-US%20Insurance%20Project/Documents/EU-US_Initiatives_2017-2019.pdf.

[3] "Regulators," as used in this paper, includes supervisory authorities. The term "insurance regulators" is intended to be synonymous with the term "insurance supervisors" used in other Project issues papers.

[4] Cyber insurance also is sometimes referred to as "cybersecurity insurance." *See, e.g.*, Memorandum from Denise Matthews, Director, Data Coordination and Statistical Analysis, to NAIC Innovation and Technology (EX) Task Force, re: Report on Cybersecurity Insurance and Identity Theft Coverage Supplement (August 6, 2018) ("NAIC Cyber Supplement Report"), https://www.naic.org/meetings1808/cmte_ex_ittf_2018_summer_nm_materials.pdf?26 (Attachment 3).

[5] *See, e.g.*, Federal Insurance Office (FIO), U.S. Department of Treasury, *Annual Report on the Insurance Industry* (2017), 54 (citations omitted), https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2017_FIO_Annual_Report.pdf.

types of cyber-related losses, including: bodily injury; property damage; intellectual property theft; reputational damage; financial theft and fraud; ransom and extortion; network security failure liability; communication and media liability; business interruption; data and software loss; fines and penalties;[6] legal defense costs; and/or incident response costs.[7] Such policies may provide coverage for both direct losses incurred by the insured as well as third-party costs. Coverage may vary depending on the policyholder's business size, with large firms more likely to procure products specifically tailored to their exposure.[8]

A. The EU and U.S. Cyber Insurance Markets

Estimating the size of the global cyber insurance market is challenging given the number of jurisdictions in which the policies are written and the many forms the policies take.[9] Most published estimates focus on stand-alone cyber insurance policies and exclude premiums collected in the form of cyber "write backs" or extensions to traditional P&C policies[10] – although, as the cyber insurance market expands and matures, such extensions could amount to a significant percentage of global cyber insurance premiums. The global stand-alone cyber insurance market was estimated at about $4.5 billion in 2017,[11] up from about $3.0 billion in 2016.[12] The U.S. market accounts for approximately 80% to 90% of the total cyber insurance market, while the EU accounts for only about 5% to 9%.[13]

In the EU, the most common types of coverage offered are business interruption and data restoration. Cyber extortion coverage, and coverage for legal support and reputational issues are also available in the EU, although to a lesser extent.

The introduction of the EU's General Data Protection Regulation (GDPR) in May 2018 has increased awareness of the risk and associated costs of data breaches and is expected to further stimulate

---

[6] Legal restrictions, however, may prohibit coverage for some fines and penalties.

[7] *See, e.g.*, RMS, *2018 Cyber Risk Outlook*, https://forms2.rms.com/CyberRiskLandscapeReport2018.html; OECD, *Enhancing the Role of Insurance in Cyber Risk* Management (2017), at 62-67 (citations omitted), https://read.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en#page61.

[8] EIOPA, *Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies* (2018) ("Structured Dialogue"), https://eiopa.europa.eu/Publications/Reports/EIOPA%20Understanding%20cyber%20insurance.pdf.

[9] *See* Section II.B, below, for a discussion of stand-alone and other types of cyber insurance.

[10] As noted above, traditional policies may exclude cyber coverage. "Write backs," in effect, undo the exclusion and affirmatively provide cyber coverage. *See, e.g.*, LMA, *Cyber Risks and Exposures: Model Clauses – Class of Business Review* (2018), https://www.lmalloyds.com/AsiCommon/Controls/BSA/Downloader.aspx?iDocumentStorageKey=c3910476-c5d4-47b1-bf3c-8b7e12e08299&iFileTypeCode=PDF&iFileName=Cyber%20Clauses%20Review.

[11] Reuters, *Global Cyber Security Insurance Market 2018 Size, Overview, Trends, Various Insurance Types, Applications, Key Player's Competitive Analysis & Growth by 2023* (May 16, 2018), https://www.reuters.com/brandfeatures/venture-capital/article?id=36676.

[12] OECD, *supra* note 5, at 60.

[13] *See* OECD, *supra* note 5, at 60. While most cyber insurance policyholders are in the U.S., many policies are written by non-U.S. insurers. Notably, the UK is a major cyber insurance center, with approximately 25% of global gross written premiums for cyber underwritten through Lloyd's syndicates in 2017, according to data from Lloyd's of London.

demand for cyber insurance in the EU.[14] More generally, the global cyber insurance market is expected to grow considerably over the coming years as awareness and understanding of cyber risks develops, with some estimates suggesting it will reach $10 billion by the end of 2020.[15]

In the U.S., state insurance regulators require all admitted insurers who write either cyber insurance or identity theft coverage to report data on such coverage in their annual reports to the National Association of Insurance Commissioners (NAIC).[16] Specifically, the Cybersecurity Insurance and Identity Theft Coverage Supplement to the Property & Casualty Annual Financial Statement (Cyber Supplement) requires insurers to report number of claims (first-party and third-party); direct premiums written and earned; direct losses paid and incurred; and number of policies in-force (claims-made and occurrence), separately reporting on both stand-alone policies and those that are part of a package policy. The NAIC recently released its report on the 2017 Cyber Supplement, reflecting information filed by approximately 500 U.S. insurers reporting $1.89 billion in direct written premium for stand-alone and package policies issued by admitted insurers, a slight increase from 2016's direct written premiums of $1.78 billion. This is the second year the NAIC received information filed by surplus lines insurers showing total premiums written for stand-alone and package policies of approximately $1.196 billion. Together, cyber insurance written in the U.S. market totaled approximately $3.1 billion.[17] Cyber insurance remains a small portion of the overall $555 billion U.S. in net written premiums reported by P&C insurers for 2017.[18]

---

[14] The GDPR requires prompt notification and disclosure of cyber events which risk the "rights and freedoms of data subjects" and individuals in the EU. *See* Regulation EU 2016/679 of the European Parliament of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.

[15] KPMG, *Seizing the Cyber Insurance Opportunity* (2017), https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/07/cyber-insurance-report.pdf.

[16] The reported information for admitted insurers is limited to those insurers required to file a P&C annual financial statement with the NAIC. To evaluate this limitation, one must understand the types of insurers writing P&C business in the U.S. and whether each type is required to report information to state insurance regulators. Generally, the U.S. regulatory system for P&C insurance views insurers as belonging in one of three classifications: (1) domestic (licensed or admitted in its selected home state or "domicile"); (2) foreign (licensed or admitted in a state but domiciled in another state); or (3) alien (not licensed or admitted in the United States). Generally, states insist insurers be licensed in the state as a prerequisite for selling products. However, states recognize that not every person or business seeking coverage for unique risks can find it from a licensed insurer. Thus, state legislatures have allowed non-licensed insurers to write P&C business under certain circumstances. The insurers doing business as non-licensed or non-admitted insurers are known as surplus lines insurers. Surplus lines insurers serve as an alternative marketplace to provide coverage for unique exposures and often serve as a testing ground for product innovations before they become mainstream. Offering coverage on a surplus lines basis allows insurers greater freedom in pricing and does not require formal prior approval by regulators of contract language.

[17] This figure includes the stand-alone and package cyber insurance premiums reported in the NAIC statutory financial statements, an estimate of the missing package cyber premiums where insurers were unable to separate cyber premiums from the package premium, and the information reported by surplus lines insurers. NAIC Cyber Supplement Report, *supra* note 2

[18] *See ,e.g.*, FIO, *Annual Report on the Insurance Industry* (2018), 84, https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2018_FIO_Annual_Report.pdf; NAIC Cyber Supplement Report, *supra* note 2; *NAIC Financial Regulatory Services P&C, Title, Life/A&H, Fraternal, and Health Industry Snapshots for the Period Ended December 31, 2017*, https://naic.org/documents/topic_insurance_industry_snapshots_2017_ye.pdf.

B. Coverage Types and Specificities

Cyber insurance policies generally fall into one of three broad categories: (1) stand-alone cyber insurance policies; (2) package coverage provided within traditional insurance products such as general liability policies; and (3) coverage provided under P&C policies that do not reference cyber coverage but lack explicit cyber exclusions, also known as "non-affirmative" or "silent" cyber risk coverage.[19]

[19] RMS, *supra* note 5.

1. Stand-Alone Cyber Insurance

Stand-alone cyber insurance products address gaps in cyber coverage resulting from cyber exclusions in traditional insurance products (such as liability, property, kidnap and ransom, and crime policies, among others). Stand-alone cyber insurance coverage varies widely: by one measure, there are at least 65 different policy forms used in stand-alone cyber policies in the U.S. alone.[20]
In the U.S., approximately 52% of cyber insurance policyholders possess stand-alone policies. Insurers writing this coverage in the U.S. reported approximately $994 million in direct written premiums in 2017, an increase of 7.99% over the prior year, spread among 45 groups of insurers (133 individual insurers). The market remains highly concentrated, with the top 10 insurers writing 79.9% of the total U.S. market, and the top 20 writing 93.2% of the market. For stand-alone cyber insurance policies sold in the U.S., the vast majority (97%) of the third-party coverage is written on a claims-made basis.[21]

2. "Package" or Endorsed Cyber Coverage

Another common means of providing cyber insurance coverage is as part of a package with a traditional insurance policy, often by policy endorsement. Coverage for cyber incidents may be packaged with traditional insurance lines such as property, directors and officers, errors and omissions/professional indemnity, general liability, crime, all-risk policies for small businesses, and homeowner policies.

In the EU, it is difficult to quantify the cyber coverage as part of package policies because such information is not collected under Solvency II reporting requirements.

Based on data filed with the NAIC, in 2017, 47% of the approximately 500 insurers who provided U.S. businesses and individuals with cyber insurance wrote cyber coverage as part of a package policy (which is a decrease from 2016 calendar year reporting, where 75% of the insurers writing cyber insurance wrote package policies). The direct written premiums for package policies sold in the U.S. were approximately $896 million.[22]

3. Non-Affirmative or Silent Cyber Coverage

Non-affirmative cyber risk is one of the key concerns for the industry and insurance regulators in both the EU and the U.S.[23] Silent or non-affirmative cyber coverage refers to policies in which cyber exposure is neither expressly excluded nor included in the policy coverage. In some cases, non-affirmative risk is

---

[20] OECD, *supra* note 5, at 62.

[21] NAIC Cyber Supplement Report, *supra* note 2.

[22] NAIC Cyber Supplement Report, *supra* note 2. The reported direct written premiums for cyber package policies totaled approximately $865 million. In 2017, 16 out of 462 insurers (i.e., 3.46% of direct written premiums for package policies) reported no premiums, generally indicating they were unable to break out the premium change for the cyber coverage from the remainder of the package policy. To arrive at a figure representing a complete market, NAIC staff assumed the 16 insurers writing cybersecurity package policies where premiums were not reported would have reported premiums in the same ratio as those insurers reporting premiums (i.e., 3.46%). The NAIC therefore estimated $31.4 million of direct written premiums for those 16 companies. As a result, by extrapolation the NAIC estimates the direct written premiums sold through package policies were approximately $896 million. *Id.*

[23] *See also* Section IV, below.

discovered only after claims disputes and/or litigation arise over cyber losses implicitly covered in traditional policies. The potential exposure from non-affirmative risk is difficult to quantify, but can be estimated through detailed assessments of the potential for cyber exposure in traditional P&C policies or via stress tests.

4. Additional Observations

Notably, in both the U.S. and the EU, many insurers now provide cyber-related services to their policyholders as a component of their cyber policies. These services include prevention programs and risk mitigation advice as well as post-breach response services.

Cyber insurance products are also being developed for individual consumers (i.e., in personal lines). For example, in the EU and U.S., cyber insurance products are now being offered to cover social media use, identity and payment card theft, online fraud and extortion, data recovery, and cyber bullying. While coverage for individual consumers is still scarce in the EU, it is perceived as a promising product as more and more individuals are exposed to cyber risks.[24]

III. Cyber insurance underwriting challenges

Underwriting cyber insurance is challenging for several reasons, including the relatively new and constantly evolving nature of the risk, the relative scarcity of loss data, and the limited availability or maturity of cyber risk catastrophe models. Historical claims data is limited, partly due to lack of reporting and partly to the short length of time cyber risk has been written. Insurers underwriting cyber risk therefore primarily rely upon qualitative models for developing policies and pricing, while robust pricing solutions are still under development by the market.

The European Insurance and Occupational Pensions Authority (EIOPA) recently conducted a structured dialogue with the EU insurance industry about cyber insurance.[25] The resulting report provides useful insights on the functioning, growth potential, challenges and risks of underwriting cyber insurance in Europe. One of the report's key findings confirms that, in light of the expected growth of the European cyber insurance market, there is a need for insurers and policyholders to deepen their understanding of cyber risk to support better underwriting and purchasing decisions. In particular, many policyholders in small and medium-sized businesses did not fully understand the products or their own needs.

According to the EIOPA report, the most frequently mentioned industry concern regarding current cyber insurance underwriting practices was the tendency of broadening coverage, terms and conditions. The key explanations provided for this tendency were increasing competition and a limited understanding of the risks. New or broader coverage may include items that are highly demanded by policyholders, but less understood by insurers from a frequency and aggregation point of view, such as systems failures (for example operational IT risk) and contingent business interruption. Several insurers stated that policy limits are driven by price rather than by the assessment of the likely indemnity required to recover the business from a cyber event. Similarly, insurers may be underwriting cyber risk based on minimal information, without the use of any modeling. As a result, there is a risk of underpricing. However, given

[24] *See, e.g.*, EIOPA, *Structured Dialogue*, *supra* note 6.

[25] EIOPA, *Structured Dialogue*, *supra* note 6.

the potential long tail risks and uncertainties around cyber risk, cyber insurance is still considered relatively expensive compared to other types of insurance coverage.

The EIOPA report also noted the treatment of contingent business interruption and the potential aggregation risk as concerns from an insurance underwriting perspective. The increase in connectivity with the centralization of IT services (for instance, the use of cloud services), and the resulting potential for increased destructiveness from cyber incidents, makes it challenging for the market to properly quantify and fund cyber risks. Misevaluation (or undervaluation) of accumulation risk may result from the lack of market standards and tools for accumulation control and risk assessment.[26]

In the U.S., a forthcoming study by the NAIC and the Center for Insurance Policy and Research (CIPR) is expected to be published by the end of 2018, *Cyber Risk Insurance: Market Advances, Challenges and Regulatory Concerns*. The study will aim to promote a more complete understanding of the unique challenges presented by cyber risk, examining the central role of the cyber insurance market, and discussing the need for and utility of further information sharing.[27] Specifically, the study is expected to discuss information asymmetry and the general lack of available data for insurers to accurately assess cyber risk and readily determine different levels of risk among current and prospective users of cyber insurance. Another challenge the NAIC/CIPR study will discuss is modeling cyber risk in a highly complex marketplace and the risks for the insurance industry related to a large-scale, catastrophic cyberattack.

IV. Supervisory practices in assessing cyber insurance underwriting

EU supervisory authorities, and U.S. state insurance regulators, have taken several steps to enhance the supervision of cyber risk underwriting. The following provides a non-exhaustive list of specific initiatives that recently have been and currently are being undertaken.

Through a Supervisory Statement published in July 2017, the U.K.'s Prudential Regulatory Authority (PRA) set out its expectations for insurance undertakings in three broad areas.[28] First, the PRA raised concerns regarding the accumulation of non-affirmative cyber risk and said it expected insurers to introduce measures that reduce the unintended exposure to non-affirmative risk within their traditional P&C contracts. Second, the PRA stressed the need for undertakings to define clear strategies and risk-appetite statements for both affirmative and non- affirmative cyber risk, with appropriate management information developed to enable monitoring of these risks at a Board level. Third, insurers are expected to continually develop their knowledge of the risk in line with their exposures and risk appetites. Following the supervisory statement's publication, the PRA held a conference to further raise awareness, especially in relation to non-affirmative cyber coverage. The PRA recognizes the challenge and accepts that insurers may require time to perform thorough risk assessments and formulate mitigating strategies. The PRA has recently conducted a follow-up exercise, asking a series of qualitative and quantitative questions to assess market movement and compliance with the expectations set out in the supervisory statement. The PRA currently is analyzing the results and intends to communicate its findings to the industry.

---

[26] EIOPA, *Structured Dialogue*, *supra* note 6.

[27] NAIC and CIPR, *Studies and Special Reports*, https://www.naic.org/cipr_special_reports.htm.

[28] PRA, *Supervisory Statement SS4/17 – Cyber Insurance Underwriting Risk* (July 2017), https://www.bankofengland.co.uk/prudential-regulation/publication/2017/cyber-insurance-underwriting-risk-ss.

In Ireland, the Central Bank of Ireland (CBI) is evolving its approach to supervising insurers offering cyber insurance. Similar to other insurance risk, the CBI's assessment centers on insurers' risk management frameworks, including whether there is Board-approved risk appetite for cyber risk; the amount of potential exposure, including from concentration and potential accumulation of incidents; whether the insurer has the necessary expertise and agility to learn from past experience and react quickly to unexpected developments; the nature of the cyber insurance product being offered (stand-alone, add-on, breach response, etc.); the type of pricing models used for the product; and what the reinsurance strategy is for the cyber insurance product. The CBI expects that any regulated entity underwriting cyber insurance would give the risk the appropriate focus in its Own Risk and Solvency Assessment (ORSA) and include adequate examination of adverse scenarios.

In the U.S., state insurance regulators use data from the NAIC Cyber Supplement to monitor cyber insurance market risk and conduct targeted examinations to the extent they see material changes in risk. Regulators use this data to identify new cyber policy writers and to monitor for any unanticipated significant increases in business written. Regulators follow up, through written inquiries or on-site examinations, to confirm that the insurer understands and is controlling the risk. Regulators review insurers' strategy, specific perils covered, exclusions, and policy limits to understand their estimated and risk capital needed to support such business under both normal and stressed situations, and how they set prices and policy terms for new cyber insurance business. As the cyber insurance market evolves, state insurance regulators remain committed to promoting an optimal regulatory framework through robust financial oversight and remaining vigilant in ensuring insurers are disciplined in their underwriting of cyber insurance products.

V. Conclusions and next steps

Going forward, Project members see the need for a deeper mutual understanding of cyber risk. Improved data collection and reporting to regulators (in the EU, in particular), as well as dissemination to the public may help insurers make better underwriting decisions and help their customers make more informed purchases. Enhanced reporting on cyber underwriting, claims, and non-affirmative exposures also is crucial for regulators to better assess insurance market risks.

In 2019, the EU-U.S. Insurance Project will continue to develop and enhance the mutual understanding of the EU and U.S. cyber insurance market and coverages and their respective regulatory frameworks. Future work may include discussions relating to:

- assessment of non-affirmative cyber risk and the potential for catastrophic losses;
- the challenges of reinsuring cyber risk; and
- the availability of cyber insurance data, including lessons learned from the experience with cyber data reporting in the U.S., and the potential for similar initiatives in the EU.