EU-US INSURANCE DIALOGUE PROJECT

THE CYBER INSURANCE MARKET WORKING GROUP
February 2020 Summary Report

I. INTRODUCTION

The EU-US Insurance Dialogue Project Cyber Insurance Working Group (WG) is pursuing an ongoing bilateral dialogue to share knowledge and experiences with respect to the development of cyber insurance markets in the United States (US) and European Union (EU). In November 2018, the Cyber Insurance WG published a paper describing the status of cyber insurance markets in the US and EU, the types of available cyber insurance coverages, challenges in underwriting cyber insurance and current supervisory practices for assessing cyber insurance underwriting.[1]

As a follow-up to the work done in 2018, the Cyber Insurance WG continued discussions with a focus on: (1) the assessment of non-affirmative cyber risk and the potential for catastrophic losses; (2) the challenges and opportunities of insuring and reinsuring cyber risk; and (3) the availability of cyber insurance data.

This report summarizes key elements of the discussions in 2019 and proposes topics for further discussion in 2020.

II. RECENT DEVELOPMENTS, CHALLENGES AND OPPORTUNITIES IN THE CYBER INSURANCE MARKET

A. Market Overview

The cyber insurance market is still relatively new and evolving and remains underdeveloped relative to other commercial insurance products on the market. The types of cyber policies offered continue to vary significantly. Further development of the cyber insurance market will likely require evolving product design that can cope with the dynamic nature of cyber risks. Overall, properly-developed insurance products and a more-developed cyber insurance market should help:

- Raise and increase awareness of cyber risks and losses among current and potential policyholders;
- Share cyber risk management best practices among stakeholders including industry, insurers, and regulators;
- Encourage the use of solid quantitative models in addition to qualitative information for effective risk-based premiums calculation; and
- Facilitate responses to and recovery from cyber incidents by policyholders.

[1] EU-U.S. Insurance Dialogue Project, *The Cyber Insurance Market* (October 31, 2018), https://www.eiopa.europa.eu/sites/default/files/publications/pdfs/the_cyber_insurance_market.pdf.

In the EU, a recent report by the European Insurance and Occupational Pensions Authority (EIOPA)[2] found that, although still small in size, the European cyber insurance industry is growing rapidly, with insurers reporting for 2018 an increase of 72% in gross written premiums,[3] amounting to EUR 295 million in 2018. As a follow up, in 2019 EIOPA developed its Cyber Underwriting Strategy highlighting EIOPA's supervisory and regulatory priorities for cyber risk. This strategy focuses on (1) appropriate cyber underwriting and cyber risk management practices including effective supervision to promote good practices, and (2) adequate assessment and mitigation tools to address potential systemic cyber and extreme risks.[4]

In the US for 2018 the total cyber insurance market was USD $ 3.6 billion; including the surplus lines market.[5] These reported direct written premiums indicate a 16.5% increase from 2017 to 2018 following a 29.5% increase from 2016 to 2017.[6] Although the pace of year-over-year growth in the US cyber insurance market has slowed, the US continues to account for the majority of the global cyber insurance market. Additionally, the US cyber insurance market is concentrated with the top ten insurers in the stand-alone and package policy market holding a supra-majority of US market share.[7]

B. Assessment of Non-Affirmative Cyber Risk and the Potential for Catastrophic Losses

Silent or non-affirmative cyber coverage refers to coverage for cyber risk under policies in which cyber exposure is neither explicitly excluded nor expressly included under policy terms. It is difficult to quantify the potential exposures from such non-affirmative cyber coverage, but estimates can be made through an examination of endorsed cyber coverage in traditional insurance policies or using stress tests. Consultations with insurers and reinsurers while developing an upcoming OECD report suggested an increasing consensus on the need to provide greater clarity on whether cyber is covered in a given policy, i.e. providing affirmative cover for – or clear exclusions of – cyber risk in each relevant line of business.

In the US, non-affirmative risk is a factor which has raised aggregation concerns and contributed to more conservative underwriting practices, given the difficulty in assessing how much it adds to an

---

[2] EIOPA, *Cyber Risk for Insurers- Challenges and Opportunities* (September 2019), https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf?source=search.

[3] The reported figures are based on the responses of 41 large (re)insurance groups across 12 European countries representing a market coverage of around 75% of total consolidated assets.

[4] https://www.eiopa.europa.eu/content/cyber-underwriting-strategy_en.

[5] In the U.S., state insurance regulators require all admitted insurers who write either cyber insurance or identity theft insurance coverage to report data on such coverage in their annual reports to the NAIC through the Cybersecurity Insurance and Identity Theft Coverage Supplement to the Property & Casualty Annual Financial Statement (NAIC Cyber Supplement). *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 (September 12, 2019) ("NAIC Cyber Supplement Report"), https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final%20%281%29.pdf.

[6] These percentages are based on the total of direct written premiums from the surplus lines market, stand-alone and package cyber insurance direct written premiums reported in the NAIC Cyber Supplement and an estimate of the missing package policy cyber insurance premiums that were not reported by insurers.

[7] *See, e.g.*, NAIC Cyber Supplement Report; Federal Insurance Office, *2019 Annual Report*, https://home.treasury.gov/system/files/311/2019_FIO_Annual_Report.pdf.

insurer's overall cyber risk portfolio. Regulators are aware of the potential risks from non-affirmative cyber exposures and have observed that insurers are continuing to update policy language to better specify coverages and exclusions. Some US insurers have indicated they will begin affirmatively covering or excluding physical and non- physical cyber exposures for most of their commercial property and casualty (P&C) policies by a specific target date. Further, some larger insurers in the US are working to create affirmative cyber programs and strengthen their underwriting strategies. These initiatives include adjusting policy language to aid in the implementation of a global affirmative underwriting approach. While still in its infancy, there has been some progress with the development of new models specifically to assess levels of non-affirmative risk and applying artificial intelligence to "read" in-force policies to detect the presence of non-affirmative risks in portfolios.On the EU side, the recent EIOPA report on cyber insurance highlighted that non-affirmative cyber exposures remain a source of concern and calls for further effort to address the issue of potential accumulation of risks. As an example, in France, the Autorité de Contrôle Prudentiel et Résolution (ACPR) has included the development of cyber insurance in its oversight priorities through the use of a self-assessment questionnaire.

In the UK, some large insurers have mandated that all non-affirmative policies provide clarity regarding cyber coverage by either expressly excluding it or affirmatively providing it. These insurers have also required that all first-party property damage policies written on or after January 1, 2020 conform to this mandate. For other lines of business, these requirements are planned to come into effect by 2021.

In general, the lack of transparency in non-affirmative exposures also creates uncertainty for policyholders, as it is often not clear whether their cyber claims would be covered by their insurance policies. Further efforts are needed to continue to address the issue of potential accumulation risk and provide greater clarity to policyholders with regards to coverage for cyber risks on a non-affirmative basis.

C. The Challenges and Opportunities of (Re)Insuring Cyber Risk

Direct writers and reinsurers face similar challenges respecting cyber business, given among other things the difficulty in quantifying cyber risk, the potential for risk accumulation and the fact that the cyber insurance landscape includes different types of policies including stand-alone policies, package policies and combinations of stand-alone and package policies. Further, changing laws and regulations in jurisdictions can also contribute to increasing variability in loss exposures.

In the EU, the ACPR has identified several challenges regarding insurance and reinsurance of cyber risks, such as the increasing magnitude of losses and the issue of correlation among risks. Furthermore, the lack of data on cyber losses has contributed to increased difficulty in measuring and forecasting losses.

In the US, limits offered for cyber risks tend to be lower than those offered for other types of property or liability insurance. Part of the reason for this is likely due to the fact that the cyber insurance market is still growing and the take-up rates for cyber insurance in the US are still relatively low.

D. The Availability of Cyber Insurance Data, including Lessons Learned from Experience with Cyber Data Reporting

The ongoing dialogue between the EU and US on cyber insurance data reporting has enabled the sharing of reporting practices and templates.

In the US, the initial cybersecurity reporting framework was established in 2015, and the US surplus lines market was added to the framework in 2016. Insurers are required to use the NAIC Cyber Supplement to report their number of claims (both first-party and third-party), direct premiums written and earned, direct losses paid and incurred, and number of policies in-force (both claims-made and occurrence), to be reported separately on both stand-alone and package policies.

Furthermore, cyber insurance data collection and analysis is part of the US Terrorism Risk Insurance Program (TRIP), which provides a backstop for certain cyber losses resulting from a certified act of terrorism. Under the annual data collection for TRIP, commercial US P&C insurers are required to report the number of policies and direct earned premiums subject to TRIP. These insurers must further indicate whether: (1) the policies were written on a stand-alone basis or as part of a package policy and (2) terrorism risk coverage was provided or declined within the cyber policy[8].

The EU shared with the US the details of the newly-introduced reporting template dedicated to cyber risk which entails requests for typical insurance data (e.g. premiums, technical provisions, etc.) as well as granular data on cyber risks description in the policies, with a split between affirmative and non-affirmative cyber risks.

On the EU side, pools for terrorism do exist at the Member States level but further discussion and investigation will be needed regarding the inclusion of cyber risks under their coverage.

III. CONCLUSIONS AND NEXT STEPS

One of the main challenges to further development of the cyber insurance markets in the US and EU relates to the limited data to appropriately assess and quantify cyber risk exposure.

Against this background, themes for further elaboration may include:

- Discussing approaches to collect data and develop techniques supporting more sophisticated assessment of cyber risks including potential accumulation risks (e.g. scenario based stress testing).

- Sharing US and EU approaches relative to cyber incident reporting and cyber incident response best practices including discussion of whether global initiatives could facilitate further understanding and underwriting of cyber risks.

- Discussing the current role and use of risk pools to provide additional capacity to tackle the potential systemic nature of cyber risk.

[8] *See* the Federal Insurance Office's 2018 *Report on the Effectiveness of the Terrorism Risk Insurance Program* (pp. 53-56), https://home.treasury.gov/system/files/311/2019_TRIP_SmallInsurer_Report.pdf and the 2019 *Study of Small Insurer Competitiveness in the Terrorism Risk Insurance Marketplace* (pp. 31-33), https://home.treasury.gov/system/files/311/2018_TRIP_Effectiveness_Report.pdf.