EU-U.S. INSURANCE DIALOGUE PROJECT

THE CYBER INSURANCE MARKET
October 2021 Summary Report

I. INTRODUCTION

The EU-U.S. Insurance Dialogue Project established in 2019 the Cyber Insurance Working Group (WG) to share knowledge and experiences with respect to the development of cyber insurance markets in the United States (U.S.) and European Union (EU).

This summary report follows up on the 2020 summary report[1] and describes discussions in the Cyber Insurance WG relating to:

- availability of cyber insurance data, including approaches to collecting data and developing techniques supporting more sophisticated assessment of cyber risks, including potential accumulation risks (e.g. scenario-based stress testing);
- approaches 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; and
- current use of risk pools to provide additional capacity to address the potential systemic nature of cyber risk.

The Cyber Insurance WG also discussed the implications of the COVID-19 pandemic for the cyber insurance market with a view to share risk assessments and experiences. This report summarizes key elements of the discussions in 2020-2021.

II. SUMMARY OF THE DISCUSSED TOPICS

A. Data Collection Approaches and Assessment of Potential Accumulation Risks

EU Updates:

EIOPA and its members in 2020 have been working on a data collection reporting template for cyber risks, which will be introduced as part of the Solvency II 2020 Review. The template represents a new introduction in the reporting package of the Solvency II framework and will allow supervisors to have a better and more detailed grasp on written premiums, technical provisions, and type and description of risks being covered.

[1] EU-US Insurance Dialogue Project, The Cyber Insurance Market Working Group February 2020 Summary Report is available at https://www.eiopa.europa.eu/content/summary-report-eu-us-insurance-dialogue-project-cyber-insurance-market-group_en. The 2020 Summary Report also discusses assessment of non-affirmative cyber risk and the potential for catastrophic losses and, challenges and opportunities of insuring and reinsuring cyber risks.

The European Commission proposed in 2020 the Digital Finance Package including a legislative proposal on digital operational resilience which will apply to all financial institutions including insurers.[2] This draft EU regulation includes standards for cyber threats, testing and reporting to supervisors.

The Central Bank of Ireland published in May 2021 the results of the Emerging Risk Survey ("The Survey"). The Survey was issued in Q4-2020 to a representative sample of 93 firms, across all sectors (life/non-life and reinsurance firms) of the insurance industry. The Survey was developed with a particular focus on climate risk (including food cover) and cyber underwriting risk. A total of 92 firms completed and returned the survey, with a response rate of 98.9%. Key findings included:

- The exposure of Irish firms to "affirmative" cyber underwriting risk appears to be limited with the share of cyber' gross written premium representing less than 1% of the total premiums written by survey respondents. For those firms that do offer cyber insurance coverage, it is typically via standalone products.
- Coverage provided focuses on commercial lines of business. The most standard types of coverage offered are business interruption, data breach, and cyber extortion coverage.
- There appeared to be challenges in disclosing cyber data. Although 32 firms indicated that they offer some type of cyber insurance cover, less than half of these were able to provide information regarding cyber-related premiums, claims and technical provisions.
- "Silent" cyber risks have not yet been fully identified – significant exposures may remain. Only 10 firms reported quantitative information of the percentage of total policy limit exposed to silent cyber risk. Even though there are some efforts from the industry to address the challenges arising from silent cyber, it appears that further work still remains to be done.

In March 2021, BaFin launched a cyber insurance survey among 60 firms (insurers, branches and reinsurance companies) which are offering cyber insurance products in Germany. The survey focused on quantitative and qualitative information such as gross and net written premiums, claims and costs and the type of coverage. A first review revealed that the cyber insurance market is significantly growing. Furthermore, the results suggest that the premium level is adequate. Since the data on cyber products are not yet subject to a separate reporting requirement, it must also be emphasized that estimates were made on the data in some cases. Partially, the system landscape of the companies was not yet able to reflect this. Nevertheless, further analysis is ongoing.

U.S. Updates:

The NAIC completed its annual Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement in the fall of 2020.[3] A report presenting 2020 data (including alien surplus

[2] The digital finance package of the European Commission published 24 September 2020 is available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684.

[3] The NAIC Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement is available at https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final_2.pdf.

lines that are reported) will be released in fall 2021. Preliminary 2020 data, focused only on cybersecurity insurance directly written by U.S. domiciled insurers, show the cyber market increased by 21.7% from 2019 to 2020, following an 11.5% increase from 2018 to 2019.

The Federal Insurance Office (FIO) also collects data on cyber insurance in its annual data call in connection with the Terrorism Risk Insurance Program and includes a summary of its findings in public reports.[4]

In January 2021, Congress enacted the William M. Thornberry National Defense Authorization Act for Fiscal Year 2021, requiring the U.S. Government Accountability Office (GAO) to conduct a study to assess the cyber insurance market. The GAO conducted the study, with input from FIO and the NAIC, noting among other things cyber insurance data trends, including increasing take up rates for cyber insurance, price increases for cyber insurance policies, and lower coverage limits for some industry sectors.[5]

There are also some private sector initiatives relative to data collection worth noting. For instance, Verisk's Cyber Data Exchange allows for participating companies to contribute their cyber insurance data into a pool and CyberAcuView plans to compile and analyze cyber related data to enhance cyber risk mitigation efforts across the insurance industry.[6]

B. Reporting Initiatives to Facilitate Further Understanding and Underwriting of Cyber Risks

The Cyber Insurance WG members from both the EU and US shared some important initiatives with regard to fostering understanding and conscious underwriting of cyber risks.

Some members of the Cyber Insurance WG, including the NAIC and FIO, participated in the drafting of the paper by the International Association of Insurance Supervisors (IAIS) on cyber risk underwriting.[7] The paper recommends that the IAIS pursue a strategic approach focusing on (1) facilitating the monitoring, understanding and assessment of cyber risk underwriting exposure and impact and (2) assisting supervisors in building relevant capacity to review cyber risk underwriting practices and exposure.

---

[4] *See, e.g.*, FIO, Report on the Effectiveness of the Terrorism Risk Insurance Program (June 2020), https://home.treasury.gov/system/files/311/2020-TRIP-Effectiveness-Report.pdf; FIO, Study of Small Insurer Competitiveness in the Terrorism Risk Insurance Marketplace (June 2021), https://home.treasury.gov/system/files/311/2021TRIPSmallInsurerReportJune2021.pdf.

[5] *See, e.g.,* GAO, Cyber Insurance – Insurers and Policyholders Face Challenges in an Evolving Market (May 2021), https://www.gao.gov/assets/gao-21-477.pdf.

[6] *See, e.g.*, Verisk, Cyber Data Exchange, https://www.verisk.com/insurance/products/cyber-data-exchange/; CyberAcuView, "Consortium of Leading Cyber Insurers Announce the Launch of CyberAcuView," press release (June 17, 2021), https://cyberacuview.com/press-release-june-2021/

[7] IAIS, Cyber Risk Underwriting: Identified Challenges and Supervisory Considerations for Sustainable Market Development (December 2020), https://www.iaisweb.org/page/supervisory-material/other-supervisory-papers-and-reports/file/94255/cyber-risk-underwriting-identified-challenges-and-supervisory-considerations-for-sustainable-market-development.

EU Updates:

EIOPA reported on its Strategy on Cyber Underwriting,[8] which represents a fundamental milestone and an important step towards the achievement of a set of specific objectives, such as:

- Appropriate cyber underwriting and risk management practices and the corresponding promotion of such practices;
- Adequate assessment and mitigation tools to address potential systemic and extreme risks;
- A mutual understanding between policyholders and insurers of contractual definitions, conditions and terms; and
- An adequate level and quality of data on cyber incidents available at the European level.

U.S. Updates:

In addition to collecting data on cyber insurance (see Section A, above), FIO also analyzes the availability and affordability of terrorism risk insurance and coverage for cyber attacks committed as an act of terrorism.[9] The NAIC Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement also includes insights into cyber insurance underwriting.[10] Some stakeholders have discussed the potential for a program similar to the Terrorism Risk Insurance Program but which would cover all cyber losses (not just those limited to terrorism); however, no legislation has been introduced to date.

As noted above, in May 2021, GAO released its report which describes key trends in the current market for cyber insurance, and identifies challenges faced by the cyber insurance market and options in order to address such challenges.[11]

On February 4, 2021, the New York State Department of Financial Services (NYDFS) issued a new Cyber Insurance Risk Framework that outlines industry best practices for New York-regulated property & casualty insurers that write cyber insurance to effectively manage their cyber insurance risk.[12] Insurers are encouraged to develop a formal risk strategy that incorporates the following: (1) manage and eliminate exposure to "silent" cyber insurance risk; (2) evaluate systemic risk; (3) rigorously measure insured risk; (4) educate insureds and insurance producers; (5) obtain cybersecurity expertise through strategic recruiting and hiring practices; and (6) require notice to law enforcement in the event of a cyber-attack. The NYDFS indicated that insurers' strategy for

---

[8] https://www.eiopa.europa.eu/content/eiopa-sets-out-strategies-cyber-underwriting-and-suptech_en.

[9] *See, e.g.*, FIO, Report on the Effectiveness of the Terrorism Risk Insurance Program (June 2020), https://home.treasury.gov/system/files/311/2020-TRIP-Effectiveness-Report.pdf.

[10] The NAIC Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement is available at https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final_2.pdf.

[11] *See* Public Law 116-283, Section 9005 (bill text available at: https://www.congress.gov/bill/116th-congress/house-bill/6395; GAO, Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market (May 2021), https://www.gao.gov/assets/gao-21-477.pdf.

[12] NYDFS, Insurance Circular Letter No. 2 (2021) (February 4, 2021), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

measuring cyber insurance risk should be directed and approved by its board or other governing entity, and should be proportionate with each insurer's risk based on the insurer's size, resources, geographic distribution, and other factors.

On June 30, 2021, NYDFS issued guidance on ransomware, noting that the rising costs of ransomware have "shaken up the cyber insurance market."[13] Based on NYDFS's investigations into reported cybersecurity events, as well as discussions with numerous experts in the field, NYDFS recommended implementation of specific cybersecurity controls which address weaknesses commonly exploited by ransomware criminals who use the same handful of techniques repeatedly. NYDFS is also considering revisions to its Cybersecurity Regulation to more thoroughly address the risks of ransomware and the evolving and more dangerous landscape that exists in 2021.

C. The Role and Use of Risk Pools to Provide Additional Capacity to Tackle the Potential Systemic Nature of Cyber Risk

The members of the Cyber Insurance WG discussed the use of risk pools as a potential resource to address the systemic nature of cyber risks. Risk pools are used for other systemic events such as terrorism, which can trigger unforeseen and significant losses. Members of the Cyber Insurance WG concluded that the use of such structures specifically for cyber risk does not seem likely in the near-term in the EU or the United States.

III. CONCLUSIONS AND NEXT STEPS

Members have identified the limited availability of data to appropriately assess and quantify cyber risk exposure as one of the main challenges to further developing the cyber insurance markets in both the U.S and EU. High level information exchanges on cyber insurance may continue within the new workstream for 2021-2022 on technology and innovation.

[13] Letter from NYDFS to All New York State Regulated Entities Re: Ransomware Guidance (June 30, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210630_ransomware_guidance.