EU-US INSURANCE DIALOGUE PROJECT

INSURER CYBERSECURITY WORKING GROUP
February 2020 Summary Report

I. INTRODUCTION: OBJECTIVES AND TARGET OUTCOME/ DELIVERABLES

The EU-US Insurance Dialogue Project's Insurer Cybersecurity Working Group objectives are:

- Keep members current as to industry developments and public sector activities within the European Union (EU) and the United States (US) with respect to cyber risks involving the insurance industry and cybersecurity efforts being taken by insurers, policymakers, and regulators.
- Share knowledge and sources as to emerging developments and best risk management, internal control, and governance practices through which insurers are managing cyber-related risks.
- Share knowledge and sources with respect to how members can address cyber risks and challenges.[1]

Building upon its 2018 work, the Insurer Cybersecurity Working Group's 2019 Target Outcome/Deliverables were:

1. Further discussions to continue to share examples and approaches to insurer cybersecurity and post-incident coordination.
2. Further discussions in moving forward with creating an outline/template for scenarios for an insurance supervisor-only exercise on how to coordinate a cross-border response in the event of an international cybersecurity incident.

II. STATUS UPDATE

A. Overview

Since its last report, the Insurer Cybersecurity Working Group held several teleconferences during which members shared information on insurer cybersecurity-related activities generally and continued discussions towards the development of an exercise template.

B. Information Sharing on Insurer Cybersecurity and Cyber Resilience

In the EU, several organizations published papers on cybersecurity risk monitoring and supervisory expectations for insurers. The Autorité de Contrôle Prudentiel et Résolution (ACPR) released a revised report on cyber resilience in January/February 2019. The ACPR also submitted a self-assessment questionnaire focusing on (1) data quality and (2) entities' information system security in

[1] These objectives are a subset of those identified for the Cyber Workstream in *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, but limited to those relevant to insurer cybersecurity. The Steering Committee formally split the "Cyber Workstream" into two working groups – (1) insurer cybersecurity and (2) the cyber insurance market – during its May 29, 2019 meeting.

order to measure the insurers' level of protection, following 2016 and 2017 surveys.[2] BaFin issued guidelines for the use of cloud computing in the financial sector, including best practices and identifying regulations that firms should take into account when using cloud-computing services. DeNederlandscheBank (DNB) published an "Information Security Monitor," as well as a "Good Practice Paper on Information Security."[3]

At the EU level, the European Supervisory Authorities (the European Banking Authority, the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority) sent joint advice to the European Commission on: (1) the need for legislative improvements relating to Information and Communication Technology (ICT) risk management requirements in the EU financial sector, and (2) the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the EU financial sector.[4] The European Commission followed up in December 2019 by launching a 12-week public consultation seeking the views of the relevant financial services community (stakeholders, national authorities, experts, and academia) on several aspects of a possible initiative on the financial sector's digital operational resilience.[5] Among other things, the consultation seeks views on the need for considering an EU-wide regulatory approach or other risk transfer schemes to ensure resilience against cyber risks. The consultation is scheduled to close on March 19, 2020, and subject to the European Commission's political validation, a potential legislative initiative may be presented by the end of 2020.

Additional reported activities in the EU related to insurer cybersecurity include the following. BaFin is intensifying its onsite inspections, as noted in its circular.[6] EIOPA developed guidelines on ICT governance for security requirements which are currently under public consultation.[7] EIOPA also is working on incident reporting from the perspective of both security and cyber underwriting and on cyber resilience testing. In addition, EIOPA published guidelines on outsourcing to the cloud, which will apply to all new or amended outsourcing arrangements effective January 1, 2021.[8] EIOPA held a first walkthrough exercise on supervisory cooperation with a national competent authority in the

[2] The questionnaire closed on November 8, 2019, but information remains available on ACPR's website at https://manager.e-questionnaire.com/questionnaire.asp?a=AmTPfnTUPP. ACPR sent the questionnaire to the entire market, including the 20 most significant entities.

[3] *See* https://www.toezicht.dnb.nl/en/binaries/51-237814.pdf and https://www.toezicht.dnb.nl/en/binaries/51-237685.pdf.

[4] EIOPA, *ESAs Publish Joint Advice on Information and Communication Technology Risk Management and Cybersecurity* (April 10, 2019), https://www.eiopa.europa.eu/content/esas-publish-joint-advice-information-and-communication-technology-risk-management-and_en?source=search.

[5] *See* European Commission, *Public Consultation: Financial Services – Improving Resilience Against Cyberattacks (New Rules)*, https://ec.europa.eu/info/law/better-regulation/initiatives/financial-services-digital-resilience-2019/public-consultation_en.

[6] *See* BaFin, *Cyber security: BaFin Survey of German Insurance Undertakings* (September 24, 2018), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2018/fa_bj_1808_Cybersicherheit_en.html.

[7] *See* EIOPA, "EIOPA consults on guidelines on Information and Communication Technology security and governance," news release, 12 December 2019, https://eiopa.europa.eu/Pages/News/EIOPA-consults-on-guidelines-on-Information-and-Communication-Technology-security-and-governance.aspx.

[8] EIOPA, *Guidelines on Outsourcing to Cloud Service Providers* (February 6, 2020)¸ https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en.

second quarter of 2019 and published its approach and lessons learned.[9] In the United Kingdom, the Prudential Regulation Authority (PRA) implemented a penetration-testing framework involving a unique exercise with one banking institution and one insurer. The PRA also published consultation papers on operational resilience (which includes resilience of information technology) and outsourcing (including cloud outsourcing).[10]

The US participated in a G7 distributed exercise in June 2019 testing communications protocols.

In the US, the Department of the Treasury and the National Association of Insurance Commissioners (NAIC) co-hosted a cybersecurity exercise in February 2019 for regional insurers in South Carolina, and another exercise in September 2019 for Kansas/Missouri regional insurers. Following the Kansas City cybersecurity tabletop exercise, NAIC staff began discussions towards drafting a set of incident response best practices. These best practices will also take into account feedback received from additional regional tabletops to be held in 2020.

Further, the NAIC adopted an insurance data security pre-breach checklist in 2019 and an insurance data security post-breach checklist for its Market Regulation Handbook to provide guidance for market conduct examinations. The pre-breach checklist provides review criteria to understand a licensee's information security program and incident response readiness. The post-breach checklist provides review criteria to understand how a licensee responded to a breach to protect consumers and eliminate the risk of a breach in the future. In addition, in 2019, the NAIC updated the Financial Condition Examiners Handbook (Handbook) to enhance cybersecurity-related guidance. The Handbook now encourages regulators to leverage cybersecurity company-completed self-assessments to guide their regulatory review. The Handbook also includes tools, such as one developed by the Financial Services Sector Coordinating Council (FSSCC) with broad support from both industry and other regulatory bodies.[11]

Finally, eight states have now implemented the NAIC's *Insurance Data Security Model Law* (Model # 668), which sets forth requirements for insurers, agents, and other licensed entities with respect to data security, breach notification, and breach investigation. Separately, the New York Department of Financial Services has implemented a cybersecurity regulation (which also helped inform the development of the NAIC's model law).

C. Exercise Template Development

In order to develop an initial cyber security exercise template (template), Working Group members are building on existing resources, such as those identified in the Project's *Insurance Industry*

[9] EIOPA, *Crisis Walkthrough Exercise: Approach and Lessons Learned* (February 7, 2020), https://www.eiopa.europa.eu/content/crisis-walkthrough-exercise-approach-and-lessons-learned.

[10] *See* PRA, Operational Resilience (CP29/19), https://hyperlink.services.treasury.gov/agency.do?origin=https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper; Outsourcing (including Cloud) (CP30/19), https://hyperlink.services.treasury.gov/agency.do?origin=https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management.

[11] FSSCP Mapping: https://content.naic.org/sites/default/files/inline-files/4-FSSCP%20Mapping%20to%20Exhibit%20C_0.xlsx.

Cybersecurity Issues Paper, rather than duplicating past efforts.[12] Members have flagged additional resources for consideration and discussed policy tools for addressing cyber incidents noting that, generally speaking, more tools are available after incidents than during incidents.

Members also have discussed parameters for the template development such as participants (e.g., what level of staff within the supervisor's office should participate), format (e.g., the relative merits of a tabletop exercise versus a distributed exercise), and scenarios. Members have acknowledged the importance of clarifying and using common terminology (e.g., "exercise template" instead of "playbook"). Members have had robust discussion about how to approach the template development. Consensus is emerging to keep the template simple so that the focus during an exercise would be on identifying where improvements are needed, rather than try to identify all issues in advance of an exercise. If this approach is followed, then there will need to be attention to developing an approach for addressing issues after the exercise, perhaps through the development of an after-action report.

III. CONCLUSIONS AND NEXT STEPS

Insurance sector cybersecurity is a continuing challenge and a matter for ongoing supervisory focus in both the US and EU. The Insurer Cybersecurity Working Group therefore recommends continuing its ongoing work:

- Continue to share information on insurer cybersecurity and operational resilience including, for example, discussing insurance industry approaches to managing cybersecurity risk; supervisory approaches to reviewing insurers' cybersecurity measures; the challenges of tracking cyber risks in the EU and the US; preventing and managing a cross-border cyber event from both a supervisory and industry perspective; and the cybersecurity implications of insurers' increased outsourcing to the cloud.

- Complete development of an initial cybersecurity exercise template for EU and US supervisors on how to coordinate a cross-border response in the event of an international cybersecurity incident. Expand current draft scenario(s) in the template, including scenario timelines with a progression of events mimicking those likely during a real cybersecurity incident. Include a list of supervisory contacts.

- Develop a timeline for conducting an exercise using the template created by the working group.

[12] EU-U.S. Insurance Dialogue Project, *Insurance Industry Cybersecurity Issues Paper* (October 2018), https://www.eiopa.europa.eu/sites/default/files/publications/pdfs/181031_eu-us_project_cybersecurity_paper_publication.pdf.