EU-U.S. INSURANCE DIALOGUE PROJECT

INSURER CYBERSECURITY
October 2021 Summary Report

I. INTRODUCTION/BACKGROUND

The EU-US Insurance Dialogue Project established the Insurer Cybersecurity Working Group to share knowledge of, and sources concerning: insurance industry developments and public sector activities within the European Union (EU) and the United States (U.S.) in connection with insurer cybersecurity; emerging developments and best risk management, internal control, and governance practices through which insurers are managing cyber-related risks; and how jurisdictions can best address cyber risks and challenges.[1] To further these objectives, in 2019 the Cybersecurity Working Group not only continued its discussions on these topics but also began 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, as previously reported.[2] In February 2020, the Cybersecurity Working Group published a summary report on its activities.[3]

In 2020, the Cybersecurity Working Group's objectives were to continue its ongoing work, including completion of the template and development of a timeline for conducting a supervisor-only cybersecurity exercise. Unfortunately, due to the COVID-19 pandemic, the activities of this Working Group were significantly curtailed, and the template remains incomplete. Working Group members, however, continued to exchange information via teleconferences and emails.

This report provides a summary of the Cybersecurity Working Group's discussions and a summary of developments in members' jurisdictions.

II. SUMMARY OF DISCUSSED TOPICS

A. Information Sharing on Insurer Cybersecurity and Cyber Resilience

Cybersecurity Working Group members shared information about activities and publications relevant to insurer cybersecurity in 2020 and 2021. Below, the report provides separate updates on U.S. and EU activities.

---

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

[2] EU-U.S. Dialogue Project, EU-U.S. Dialogue Project: Insurance Cybersecurity Working Group February 2020 Summary Report (February 2020), https://www.eiopa.europa.eu/sites/default/files/publications/eu-us-project-cybersecurity-wg-feb-2020.pdf.

[3] Id.

Project members, however, are also engaged in relevant activities at the International Association of Insurance Supervisors (IAIS) and the Financial Stability Board (FSB). Notably, in this regard, the IAIS formed the Operational Resilience Task Force which will develop supervisory guidance and material, as appropriate, on information technology, third-party outsourcing, and insurance sector cyber resilience, among other things.[4] The FSB published a consultation report on Effective Practices for Cyber Incident Response and Recovery, which was sent to G20 Finance Ministers and Central Bank Governors for their virtual meeting on April 15, 2020. The toolkit of effective practices aims to assist financial institutions in their cyber incident response and recovery activities.[5]

U.S. Updates

The U.S. Cyberspace Solarium Commission published a report in March 2020 with its proposed strategy for cyber deterrence through 80 recommendations which included—but were not limited to—recommendations about cyber insurance.[6]

The Federal Insurance Office (FIO) published its Annual Report on the Insurance Industry in September 2020. The report discussed insurer cybersecurity, including in the context of the COVID-19 pandemic.[7] FIO's 2021 Annual Report, published on September 30, 2021, also discusses insurer cybersecurity.[8]

In 2021, the federal government responded to the increasing frequency and severity of ransomware attacks with additional cybersecurity measures which are applicable to insurers (and other sectors). On July 15, 2021, the U.S. Department of Homeland Security and U.S. Department of Justice launched StopRansomware.gov, a website with advice and resources for combatting ransomware threats.[9] The U.S. Department of State established a Rewards for Justice program, in which it offers a reward of up to $10 million for information leading to the identification or location of a person who participates in cyber-intrusions, including ransomware, against U.S. critical infrastructure.[10] On August 25, 2021, President Biden hosted a summit with the private sector to discuss opportunities to bolster the nation's cybersecurity capabilities, including how the cyber

---

[4] IAIS, 2021-2022 Roadmap (adopted February 22, 2021), www.iaisweb.org/page/about-the-iais/public-roadmap//file/95571/2021-2022-iais-public-roadmap.

[5] https://www.fsb.org/2020/04/fsb-consults-on-effective-practices-for-cyber-incident-response-and-recovery/.

[6] *See* "United States of America Cyberspace Solarium Commission," https://www.solarium.gov/.

[7] FIO, Annual Report on the Insurance Industry (September 2020), 33-34, 71-73, https://home.treasury.gov/system/files/311/2020-FIO-Annual-Report.pdf.

[8] FIO, Annual Report on the Insurance Industry (September 2021), 77-80, https://home.treasury.gov/system/files/311/FIO-2021-Annual-Report-Insurance-Industry.pdf.

[9] U.S. Department of Justice, "U.S. Government Launches First One-Stop Ransomware Resource at StopRansomware.gov," news release (July 15, 2021), https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov.

[10] U.S. Department of State, "Rewards for Justice – Reward Offer for Information on Foreign Malicious Cyber Activity Against U.S. Critical Infrastructure," news release (July 15, 2021), https://www.state.gov/rewards-for-justice-reward-offer-for-information-on-foreign-malicious-cyber-activity-against-u-s-critical-infrastructure/.

insurance market could be leveraged to combat rising ransomware threats.[11] On September 21, 2021, Treasury announced that it had taken robust actions to counter ransomware: among other things, Treasury's Office of Foreign Assets Control (OFAC) released an updated advisory on potential sanctions risk for facilitating ransomware payments.[12]

The NAIC recognizes the expanding influence and role of technology and innovation on the insurance market and is taking the significant step of creating a new standing committee focused on innovation, artificial intelligence (AI) and cybersecurity by the end of this year. While the mission and charges of the new H committee have not yet been finalized, it will likely be charged with monitoring developments and coordinating the NAIC's work in the areas of innovation, AI, and cybersecurity that are impacting the insurance sector. The new committee will also determine an appropriate approach to developing regulatory models and guidance, as deemed necessary, to ensure the state-based system continues to keep pace with the rapidly evolving insurance sector.

The NAIC is also working with state regulators to host a ransomware themed table top exercise in November 2021 in Connecticut. As of September 2021, there were 76 confirmed participants including state insurance regulators, local and regional insurers and law enforcement including the FBI, Homeland Security (CISA), and the Connecticut cyber task force. The NAIC plans to organize further table tops with other states into 2022.

U.S. states also have been responding to cybersecurity threats against insurers. On June 30, 2021, the New York Department of Financial Services (NYDFS) issued guidance in a letter to the financial services sector—including the insurance sector—to address the increasing threats of ransomware.[13] The guidance includes nine security controls that NYDFS expects regulated companies to implement where possible under the state's cybersecurity regulation.[14] The recommended controls are: (1) filter emails and provide anti-phishing training to all employees; (2) maintain documented vulnerability and patch management policies which include periodic penetration testing and require timely remediation of vulnerabilities; (3) use multi-factor authentication for remote access to internal networks and all externally exposed enterprise and third-party applications, as well as for all privileged accounts whether accessed remotely or internally; (4) disable Remote Desk Protocol access from the internet wherever possible; (5) use strong, unique passwords, and consider a password vaulting solution; (6) carefully manage privileged access by ensuring each privileged user is provided the least privileged access necessary to do a job; (7) implement a system to monitor for anomalous activity and respond to alerts of suspicious activity; (8) segregate back-ups and periodically test to make sure systems can be restored from them; and (9) ensure incident response plans explicitly address ransomware attacks.

---

[11] *See, e.g.*, "What Insurance Firms Promised at the White House Cybersecurity Summit," Insurance Journal (August 26, 2021), https://www.insurancejournal.com/news/national/2021/08/26/628904.htm.

[12] U.S. Department of the Treasury, "Treasury Takes Robust Actions to Counter Ransomware," news release, (September 21, 2021), https://home.treasury.gov/news/press-releases/jy0364.

[13] NYDFS, "Superintendent Lacewell Announces DFS Issues New Guidance on Ransomware Prevention," news release, June 30, 2021, https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202106302.

[14] NYDFS, "Ransomware Guidance," June 30, 2021, https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210630_ransomware_guidance.

In addition, the NYDFS issued a Cyber Insurance Risk Framework in an effort to foster a robust cyber insurance market that maintains financial stability and protects consumers.[15] The Framework calls on insurers to, among other actions, establish a formal cyber risk strategy, evaluate and measure systemic risk, and require victims to report cyber-attacks to law enforcement.[16]

As of 2021, at least eighteen states have adopted, in a substantially similar way, the NAIC Insurance Data Security Model Law.[17] In addition, NYDFS has implemented a cybersecurity regulation which also helped inform the development of the NAIC's model law.[18] According to NAIC data, 82 percent of the U.S. insurance market (as measured by gross written premium filed with the NAIC) is subject to the NAIC Insurance Data Security Model Law requirements or similar requirements. In July 2020, the NYDFS filed its first enforcement action under its cybersecurity regulation, alleging that a title insurer improperly failed to protect customer data.[19] The NYDFS has continued to bring enforcement actions against insurers under its cybersecurity regulation.[20]

EU Updates

In October 2020 EIOPA published guidelines on Information and Communication Technology (ICT) governance for security requirements which came into force in July 2021.[21] The objective of the guidelines is to promote the increase of operational resilience in the digital operations of insurance and reinsurance companies against the risks they face. Operational resilience is key to protecting insurance and reinsurance undertakings' digital assets, including their systems and data from policyholders and beneficiaries. By providing clarification and transparency to market participants on the minimum expected information and cyber security capabilities (i.e., a security baseline), the guidelines will help avoid potential regulatory arbitrage and foster supervisory convergence regarding the expectations and processes applicable in relation to ICT security and governance as a key to proper ICT and security risk management.

---

[15] NYDFS, "Cyber Insurance Risk Framework," February 4, 2021, https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

[16] NYDFS, "Cyber Insurance Risk Framework."

[17] *See* Insurance Data Security Model Law, https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf.

[18] *See* "Cybersecurity Resource Center," https://www.dfs.ny.gov/industry_guidance/cybersecurity.

[19] *See* NYDFS, "Department of Financial Services Announces Cybersecurity Charges Against a Leading Title Insurance Provider for Exposing Millions of Documents with Consumers' Personal Information," news release, 22 July 2020, https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202007221.

[20] *See* NYDFS, "DFS Superintendent Lacewell Announces Cybersecurity Settlement with First Unum and Paul Revere Life Insurance Companies," news release, May 13, 2021, https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202105131; NYDFS, "DFS Superintendent Lacewell Announces Cybersecurity Settlement with Licensed Insurance Company," news release, April 14, 2021, https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202104141; Consent Order, In the Matter of National Securities Corporation, April 12, 2021, https://www.dfs.ny.gov/system/files/documents/2021/04/ea20210412_national_securities_corp.pdf.

[21] *See* EIOPA, "EIOPA finalizes Guidelines on Information and Communication Technology Security and Governance," news release, 12 October 2020, https://www.eiopa.europa.eu/content/eiopa-finalises-guidelines-information-and-communication-technology-security-and-governance_en?source=search.

B. Exercise Template Development

The Cybersecurity Working Group continued to discuss the assumptions and recommendations in the draft template, to verify consensus on key points, including, for example:

- **Participants**: Cybersecurity Working Group members discussed at length the target number of participants, and suggested that the target might preferably be approximately 30-35 participants (assuming 2-3 representatives for approximately 10-12 participating entities).

- **Surprise vs. Prepared Exercise**: Members also discussed the pros and cons of providing the participants with full scenario details in advance vs. providing no advance details (or providing only the initial scenario and not the further scenario developments for later in the exercise). EU members were more familiar with "surprise" exercises, which would be closer to a real-time crisis simulation; while U.S. members were more familiar with a prepared exercise which could permit more planning and more structure. A compromise approach could be to run two exercises: (1) a prepared exercise in which the participants could fully discuss their different approaches to a cybersecurity incident, to be followed, after a reasonable interval, by (2) a separate real-time "surprise" simulation.

- **Scenarios**: Members agreed that there should be a single, evolving scenario rather than multiple scenarios. Members highlighted where the current high-level scenario examples should be fleshed out.

- **Recaps**: Members agreed that while the exercise itself might include an initial recap, it should be clear that there would be a separate, follow-on discussion about the exercise.

Given the constraints imposed by the pandemic, the Cybersecurity Working Group has paused its development of the template and exercise planning.

III. CONCLUSION

Insurance sector cybersecurity is a continuing challenge and a matter for ongoing supervisory focus in both the United States and the European Union. The Project has served an important role in forging staff-level connections across the Atlantic, and opening up important lines of communication. The Project's Steering Committee, however, has determined that other emerging issues will be the focus for bilateral discussions in 2021 and 2022. High-level cyber-related issues can still be flagged in the 2021-2022 technology and innovation workstream.