Draft: 9/11/24

Cybersecurity (H) Working Group
Virtual Meeting
September 4, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met September 4, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Chris Erwin (AR); Bud Leiner (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Matt Kilgallen (GA); Lance Hirano (HI); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Mary Kwei (MD); Jake Martin (MI); T.J. Patton (MN); Tracy Biehn (NC); Colton Schulz (ND); Martin Swanson (NE); Christian Citarella (NH); Scott Kipper (NV); Gille Ann Rabbin (NY); Don Layson (OH); David Buono (PA); Bryon Welch (WA); Andrea Davenport (WI); and Lela Ladd (WY).

1. Adopted its Summer National Meeting and Aug. 1 Minutes

The Working Group met Aug. 1 and took the following action: 1) heard an update from Shana Oppenheim (NAIC) regarding her observations of federal cybersecurity and cyber insurance activities.

Schulz made a motion, seconded by Buono, to adopt the Working Group's Aug. 14 (*see NAIC Proceedings, Summer 2024 – Innovation, Cybersecurity, and Technology (H) Committee, Attachment Three*) and Aug. 1 (Attachment One) minutes. The motion passed unanimously.

2. Heard a Presentation from AM Best on the Cyber Insurance Market

Michael Lagomarsino and Tom Mount (AM Best) gave an informational presentation to the Working Group on the U.S. cyber market and AM Best's cyber initiatives. Lagomarsino said AM Best assigned a stable outlook on the global cyber insurance market. Some of the positive factors supporting that outlook include continued demand, increasing take-up rates for cyber insurance coverage, and continual improvements in cyber hygiene. Greater take-up rates, primarily in small and medium enterprises (SMEs), will drive growth over the next five to ten years. He said improvements in underwriting practices and risk selection practices of insurers have driven investments in cyber security. Additionally, cyber insurance turned to incorporating exclusionary language around critical infrastructure and war as an action to reduce exposure to aggregate losses. Lagomarsino said the market has been supported by reinsurance, with roughly 50% of premium ceded to reinsurance. Several cyber catastrophe bonds have been issued over the last 12 months on the public market. This is a positive sign that investors are getting more comfortable with how cyber is being underwritten.

Lagomarsino introduced several countervailing factors the global cyber insurance marketplace faces, including increased competitive pressure and additional capacity entering the market. AM Best is watching how the market responds to recent high-profile cyberattacks; however, to date, insured losses from these recent incidents appear manageable. The attacks serve as a reminder of uncertainty over the aggregation of risk, the growing sophistication of attacks using artificial intelligence (AI), and the dynamic nature of the cyber risk environment. Lagomarsino explained that any reduction in reinsurance capacity would reflect a reduction in cyber risk appetite on the primary side, which could result in significant market dislocation.

Discussing trends observed in the U.S. cyber insurance market, Lagomarsino explained that there was a deterioration in the direct loss and defense and cost containment (DCC) loss ratio, driven by a significant increase in the frequency of ransomware attacks at the onset of the COVID-19 pandemic. Companies aggressively invested in technology to enable remote work environments, leading to significant losses. Insurance companies reacted with significant rate increases while tightening terms and conditions, specifically increasing deductibles and putting sub-limits within the policies. The aggressive actions, in conjunction with improved cybersecurity hygiene, resulted in significant improvement in underwriting results. Lagomarsino observed that premiums experienced significant growth in 2022 and flattened in 2023, but profitability remains strong and is expected to remain in place for the foreseeable future. Citing a report by Howden, he added that global cyber insurance premiums are three times higher than pre-COVID levels; however, they have flattened and are even turning negative more recently. Summarizing post-COVID trends in cyber claims, Lagomarsino stated that year-over-year (YOY) growth has been driven by first-party claims, which tend to be shorter-tailed in nature and enable carriers to respond quicker. He said the increased frequency of ransomware attacks since the COVID-19 pandemic continued to hit record levels in 2023. Due to improved cybersecurity hygiene, though, the percentage of companies impacted by a ransomware attack that are paying the ransom has significantly come down over time, which should reduce claim severity.

Mount delivered a detailed overview of AM Best’s credit rating methodology and the building block approach. He explained rating considerations for affirmative cyber and highlighted some areas of a balance sheet that cyber would affect. He described why incorporating catastrophe risk and stress testing is necessary and could effectively manage exposure to catastrophe events, which is essential to protecting and preserving balance sheet strength. Mount gave examples of how catastrophe modeling could look at historical losses and conduct deterministic scenarios for estimating loss. He described a cyber catastrophe as a shock loss, which is usually a large and sudden loss with a shorter tail. Additionally, he said some challenges for cyber stress testing are in how various models differ. While some have similar assumptions, others might better capture a certain type of exposure or risk.

Mount explained the AM Best team is developing a cyber questionnaire to help understand the growth in affirmative cyber writing and to quantify and understand the impact of cyber risk management. The general questions he described sought to answer the nature of the portfolio, cyber risk appetite, and underwriting strategy to better understand the use of third parties.

Concluding their presentation, Lagomarsino explained that many companies manage cyber risks through underwriting and risk transfer as well as through policy wording, like the war exclusions. He described companies as being mindful of the rate component versus the terms and conditions, as they are focusing on managing their aggregates in the underwriting process.

In recognition of the elapsed time, Amann suggested that the meeting's question-and-answer (Q&A) portion be skipped to allow the vice chair to discuss a requested update. She expressed appreciation for the guest speakers and welcomed Peterson to address the Working Group.

3. Received a Chief Financial Regulator Forum Referral

Amann informed the Working Group to expect an email following the meeting to discuss the referral received by the Chief Financial Regulator Forum.

4. Discussed Other Matters

Peterson gave an update on the activities following the adoption of the Cybersecurity Event Response Plan (CERP), which is developing a confidential repository for cybersecurity event notification. The CERP is intended to be guidance for departments of insurance (DOIs) when they must respond to a cybersecurity event. Peterson explained that the building of a notification portal requires that the state insurance regulators achieve agreement on two primary concerns: 1) whether it will meet the needs of the state that has passed its own version of the *Insurance Data Security Model Law* (#668); and 2) whether it will fill the confidentiality and security commitments made to the industry. Peterson discussed the Model #668 survey under development and offered the idea of a proof of concept as a step to provide the necessary understanding. He suggested the Working Group ask NAIC staff to build a narrowly scoped notification portal for initial assessment. Peterson said it would be accessible initially to the states with their own version of Model #668, and the initial fit would be those questions in Section 6B. Peterson said the proof of concept and the survey to the states should give state insurance regulators an understanding of the confidentiality and security measures expected in order to pass a formal motion to begin the testing and future implementation of the portal.

Amann suggested a Working Group call in the future to discuss the Model #668 survey and notification portal project.

Having no further business, the Cybersecurity (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Fall/WG-Cybersecurity/2024 0904 Interim-Meeting/Minutes-CyberWG090424.docx