Update on the Federal Insurance Office's Work to Assess a Potential Federal Insurance Response to Catastrophic Cyber Incidents

Presentation to Advisory Committee on Risk-Sharing Mechanisms
August 1, 2024

Introduction and Background

- FIO last briefed the Advisory Committee on Risk-Sharing Mechanisms (ACRSM) on the joint assessment of a potential federal insurance response to catastrophic cyber incidents at ACRSM's February 1, 2024 meeting. This presentation provides a brief update on recent developments.
- FIO and the Cybersecurity and Infrastructure Security Agency (CISA) launched the joint assessment in June 2022 and completed the first phase of the assessment, determining whether a federal response is warranted, in December 2023.
- In 2024, FIO and CISA began the second phase of the assessment – exploring the appropriate *form* that a federal insurance response to catastrophic cyber incidents might take. On May 16th FIO hosted an initial conference on that subject.
- The conference featured remarks by senior officials from Treasury, CISA, and the Office of the National Cyber Director (ONCD). It also featured three panels with senior insurance industry cyber executives/experts from major insurers, reinsurers, and brokers. Two of the panel moderators were from cyber modeling firms.

May 16, 2024 Treasury Conference Exploring Potential Forms of a Federal Insurance Response to Catastrophic Cyber Incidents

Remarks by CISA's Associate Chief of Policy Elke Sobieraj

***Panel 1: Estimating the Protection Gap**: Scope of Coverage, the Current and Future Size of the Cyber Insurance Market, Exclusions for War/State-Supported Attacks and Infrastructure, and Potential Catastrophic Cyber Losses*

- John Farley, Cyber Practice Group Leader, **Arthur J. Gallagher**
- Bob Wice, Head of Underwriting Management Cyber Risks, **Beazley**
- Matt Prevost, Chief Underwriting Officer, Global Cyber, **Chubb**
- Damini Mago, Assistant Director, Cyber, **Moody's RMS** (moderator)

Remarks by Treasury's Acting Assistant Secretary for Financial Institutions Laurie Schaffer

***Panel 2: Considering Various Federal Reinsurance Structures** As One Potential Form of a Federal Insurance Response to Catastrophic Cyber Incidents*

- Crystal Boch, Senior Director, US Cyber Analytics, **Aon**
- Lori Bailey, Head of Global Cyber & Technology, **AXIS Capital**
- Erica Davis, Global Co-Head of Cyber, **Guy Carpenter/Marsh McLennan**
- Monique Ferraro, Cyber Counsel, **HSB/Munich Re**
- Pascal Millaire, CEO, **CyberCube** (moderator)

***Panel 3: Broader Thoughts on Catastrophic Cyber Risk**, and Other Potential Responses Other than Federal Reinsurance, Including Non-Responses*

- John Seo, CEO, **Fermat Capital Management**
- Patrick Davison, Head of Underwriting Solutions, **Lloyd's**
- Marc Amen, President, **Renaissance Reinsurance U.S.**
- Andreas Schmitt, Global Cyber Underwriting Manager, **Zurich**

Remarks by ONCD's Assistant National Cyber Director Nick Leiserson

Estimating the Protection Gap: Scope of Coverage, the Current and Future Size of the Cyber Insurance Market, Exclusions for War/State-Supported Attacks and Infrastructure, and Potential Catastrophic Cyber Losses

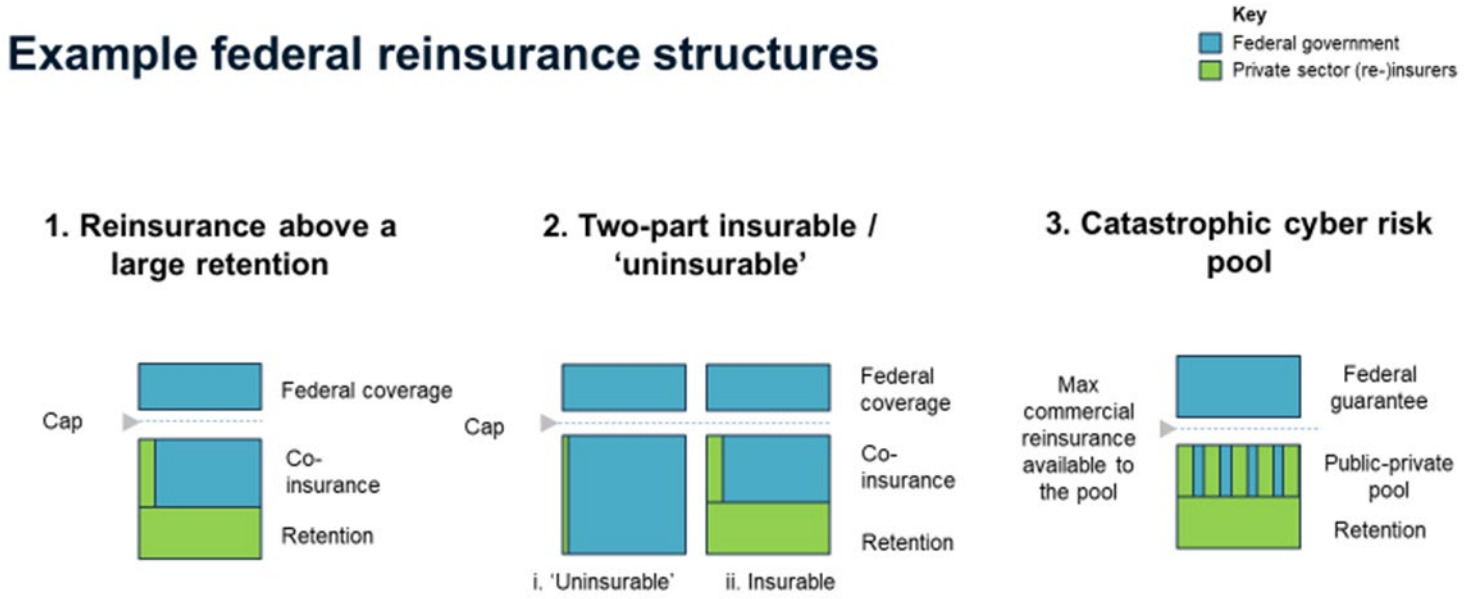
The first panel set the stage for the conference by estimating the potential catastrophic cyber protection gap. In addition, the panel provided estimates and projections of the current and future size of the cyber insurance market. The panel also discussed scope of coverage, catastrophic cyber loss models, and the state of exclusions for war/state-supported attacks and infrastructure.

Although the panelists shared a range of estimates and views, there was general agreement that there is a growing catastrophic cyber protection gap.

Considering Various Federal Reinsurance Structures As One Potential Form of a Federal Insurance Response to Catastrophic Cyber Incidents

During the second panel, the moderator provided concrete illustrations of what a federal insurance response could look like in practice. For the sake of discussion, the panel stipulated that a potential federal insurance response might take the form of a reinsurance structure. The panel discussed a handful of broad-stroke, but distinct, approaches, all of which featured some degree of public-private risk-sharing.

The panel 2 moderator (CyberCube) created and displayed this diagram of three possible federal reinsurance approaches:



Broader Thoughts on Catastrophic Cyber Risk, and Other Potential Responses Other than Federal Reinsurance, Including Non-Responses

The third panel focused on potential responses to catastrophic cyber risk, other than a reinsurance structure, including an option to not respond at all. The positions discussed ranged from “Should the federal government do nothing regarding catastrophic cyber risk narrowly defined?” (at one end of the spectrum) to “Should the federal government handle all catastrophic cyber risk as broadly defined?” (at the other end of the spectrum).

Not surprisingly, most of the discussion took place between the two extremes, although the idea that the cyber market is sufficiently new that the government should adopt a “wait and see” approach had some support.

There was recognition that the capital markets are starting to take on some catastrophic cyber risk as insurance-linked securities (ILS) markets issue cyber cat bonds, but also recognition that most catastrophic cyber risk remains uncovered, and that coverage of this risk probably requires some kind of public-private collaboration.