GAO@100 Highlights

Highlights of GAO-21-477, a report to congressional committees

May 2021

CYBER INSURANCE

Insurers and Policyholders Face Challenges in an Evolving Market

Why GAO Did This Study

Malicious cyber activity poses significant risk to the federal government and the nation's businesses and critical infrastructure, and it costs the U.S. billions of dollars each year. Threat actors are becoming increasingly capable of carrying out attacks, highlighting the need for a stable cyber insurance market.

The National Defense Authorization Act for Fiscal Year 2021 includes a provision for GAO to study the U.S. cyber insurance market. This report describes (1) key trends in the current market for cyber insurance, and (2) identified challenges faced by the cyber insurance market and options to address them.

To conduct this work, GAO analyzed industry data on cyber insurance policies; reviewed reports on cyber risk and cyber insurance from researchers, think tanks, and the insurance industry; and interviewed Treasury officials. GAO also interviewed two industry associations representing cyber insurance providers, an organization providing policy language services to insurers, and one large cyber insurance provider.

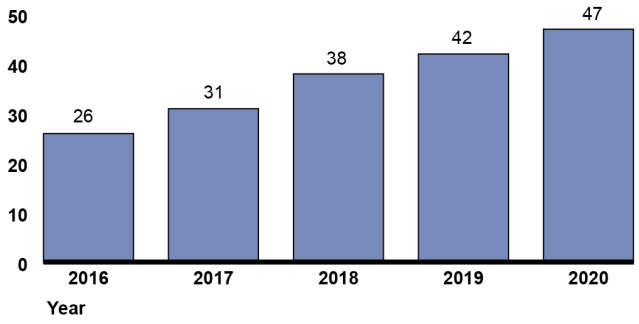
View GAO-21-477. For more information, contact John Pendleton at (202) 512-8678 or pendletonj@gao.gov.

What GAO Found

Key trends in the current market for cyber insurance include the following:

- **Increasing take-up.** Data from a global insurance broker indicate its clients' take-up rate (proportion of existing clients electing coverage) for cyber insurance rose from 26 percent in 2016 to 47 percent in 2020 (see figure).
- **Price increases.** Industry sources said higher prices have coincided with increased demand and higher insurer costs from more frequent and severe cyberattacks. In a recent survey of insurance brokers, more than half of respondents' clients saw prices go up 10–30 percent in late 2020.
- **Lower coverage limits**. Industry representatives told GAO the growing number of cyberattacks led insurers to reduce coverage limits for some industry sectors, such as healthcare and education.
- **Cyber-specific policies**. Insurers increasingly have offered policies specific to cyber risk, rather than including that risk in packages with other coverage. This shift reflects a desire for more clarity on what is covered and for higher cyber-specific coverage limits.

Cyber Insurance Take-up Rates for a Selected Large Broker's Clients, 2016–2020



Source: GAO presentation of data from Marsh McLennan. | GAO-21-477

The cyber insurance industry faces multiple challenges; industry stakeholders have proposed options to help address these challenges.

- **Limited historical data on losses.** Without comprehensive, high-quality data on cyber losses, it can be difficult to estimate potential losses from cyberattacks and price policies accordingly. Some industry participants said federal and state governments and industry could collaborate to collect and share incident data to assess risk and develop cyber insurance products.
- **Cyber policies lack common definitions**. Industry stakeholders noted that differing definitions for policy terms, such as "cyberterrorism," can lead to a lack of clarity on what is covered. They suggested that federal and state governments and the insurance industry could work collaboratively to advance common definitions.