June 2022

CYBER INSURANCE

Action Needed to Assess Potential Federal Response to Catastrophic Attacks

GAO Highlights

Highlights of GAO-22-104256, a report to congressional committees

Why GAO Did This Study

Cyber threats to critical infrastructure represent a significant economic challenge. Although cyber incident costs are paid in part by the private cyber insurance market, growing cyber threats have created uncertainty in this evolving market.

The Further Consolidated Appropriations Act, 2020, includes a provision for GAO to study cyber risks to U.S. critical infrastructure and available insurance for these risks. This report examines the extent to which (1) cyber risks for critical infrastructure exist; (2) private insurance covers catastrophic cyber losses and TRIP provides a backstop for such losses; and (3) cognizant federal agencies have assessed a potential federal response for cyberattacks.

GAO reviewed cyber insurance coverage literature and reports on cyber risk and the insurance market. GAO interviewed CISA and FIO officials and industry stakeholders (e.g., critical infrastructure owners, insurers, and brokers) that were selected based on factors such as expertise and market share.

What GAO Recommends

CISA and FIO should jointly assess the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response, and inform Congress of the results of their assessment. Both agencies agreed with the recommendations.

View GAO-22-104256. For more information, contact Daniel Garcia-Diaz at (202) 512-8678 or garciadiazd@gao.gov, or Kevin Walsh at (202) 512-6151 or walshk@gao.gov.

What GAO Found

U.S. critical infrastructure (such as utilities, financial services, and pipelines) faces increasing cybersecurity risks. Understanding these risks and associated vulnerabilities, threats, and impacts is essential to protecting critical infrastructure.

Cybersecurity Vulnerabilities, Threats, and Impacts
Vulnerabilities. Critical infrastructure has become more vulnerable to cyberattacks for reasons that include greater use of interconnected electronic systems.
Threats. Threat actors—such as nation-states, criminal groups, and terrorists—have become increasingly capable of carrying out cyberattacks on critical infrastructure.
Impacts. Federal and industry data indicate that cyberattacks—including those affecting critical infrastructure—generally have increased in frequency and cost.

Source: Prior GAO reports and GAO analysis of agency and industry documentation.

The effects of cyber incidents can spill over from the initial target to economically linked firms—magnifying damage to the economy. For example, in May 2021 the Colonial Pipeline Company learned that it was the victim of a cyberattack that led to short-lived gasoline shortages.

Cyber insurance and the Terrorism Risk Insurance Program (TRIP)—the government backstop for losses from terrorism—are both limited in their ability to cover potentially catastrophic losses from systemic cyberattacks. Cyber insurance can offset costs from some of the most common cyber risks, such as data breaches and ransomware. However, private insurers have been taking steps to limit their potential losses from systemic cyber events. For example, insurers are excluding coverage for losses from cyber warfare and infrastructure outages. TRIP covers losses from cyberattacks if they are considered terrorism, among other requirements. However, cyberattacks may not meet the program's criteria to be certified as terrorism, even if they resulted in catastrophic losses. For example, attacks must be violent or coercive in nature to be certified.

The Department of the Treasury's Federal Insurance Office (FIO) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) both have taken steps to understand the financial implications of growing cybersecurity risks. However, they have not assessed the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response. CISA is the primary risk advisor on critical infrastructure and FIO the federal monitor of the insurance sector. Accordingly, they are well-positioned to jointly perform such an assessment. Doing so and reporting the results to Congress can inform deliberations on whether a federal insurance response is warranted.

If such a response were deemed necessary, GAO's framework for providing federal assistance to private market participants (GAO-10-719) could help inform its design. The framework notes the need to define the problem, mitigate moral hazard (that the existence of a federal backstop could result in entities taking greater risks), and protect taxpayer interests. Consistent with these elements, any federal insurance response should include clear criteria for coverage, specific cybersecurity requirements, and a dedicated funding mechanism with concessions from all market participants.