Commercial Cyber Insurance Market Survey Report

August 2024

American Property Casualty Insurance Association℠
INSURING AMERICA apci.org

THE COUNCIL
The Council of Insurance Agents & Brokers

0824 | 3644PA

EXECUTIVE SUMMARY

Most cyber insurance gaps may be filled, though it could take more than three years to address some of those gaps in the provision of cyber insurance to businesses and other organizations, and sectors ranging from utilities to higher education could be challenged in securing coverage at all, according to survey findings from two leading insurance industry associations.

Earlier this year, members of the American Property Casualty Insurance Association (APCIA) who write cyber insurance were invited to respond to a survey regarding marketplace gaps in coverage or risk selection in the cyber insurance market.

Working in tandem with the APCIA, The Council of Insurance Agents & Brokers (Council) also surveyed a sample of domestic broker members and their leads on cyber insurance placements using similar questions regarding cyber policy limits, claims, gaps in coverage, and industry challenges.

MARKETPLACE GAPS IN CYBER INSURANCE

Seventy-five percent of respondents to the APCIA survey said they expect many of today's marketplace gaps in coverage or risk-selection to be addressed in the long-term (more than three years). While Council respondents were mixed in whether such gaps would be addressed in the long-term, they believe the market will address coverage limit adequacy, cyber-related physical damage, and security breach liability coverages in the short-term (within the next three years).

Sectors identified in one or both surveys as facing difficulties in obtaining cyber insurance encompass government entities, utilities, education, cryptocurrency, and food and beverage, among others.

To acquire cyber insurance, businesses may first need to implement minimum cybersecurity practices, such as multifactor authentication. Among APCIA respondents, approximately 69% are aware of applicants that had requested but were unable to obtain cyber insurance because they did not have minimum best practices in place. Likewise, 69% of Council respondents indicated they know of instances in which cyber insurance was requested but not provided for the same reason.

CATASTROPHIC CYBER EVENT

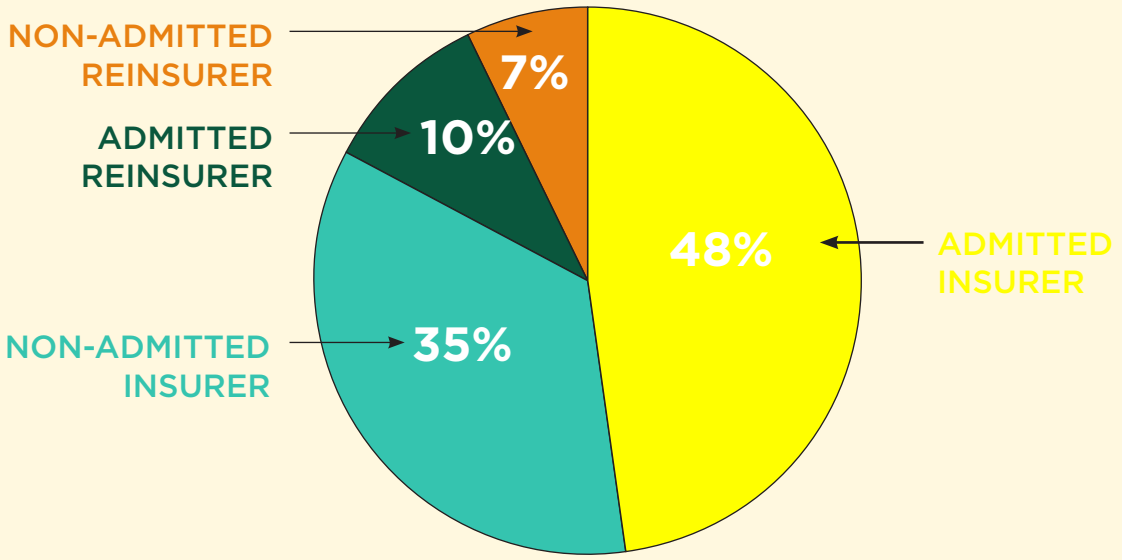
Various parameters may be considered in defining a catastrophic cybersecurity event, including impacts to critical infrastructure and on certain industries such as finance, telecom, and logistics. Council respondents identified total damages, impacts to a specific industry, and the cause/nature of an event as the most important factors in identifying a catastrophic cyber event.

APCIA respondents offered a wide range of potential loss thresholds for defining a catastrophic cyber event. Some observed that providing such a threshold is difficult and would vary depending on the size and revenue of the business affected by a cyber event, i.e., a small business's cyber event would not necessarily be catastrophic to a multibillion-dollar corporation.

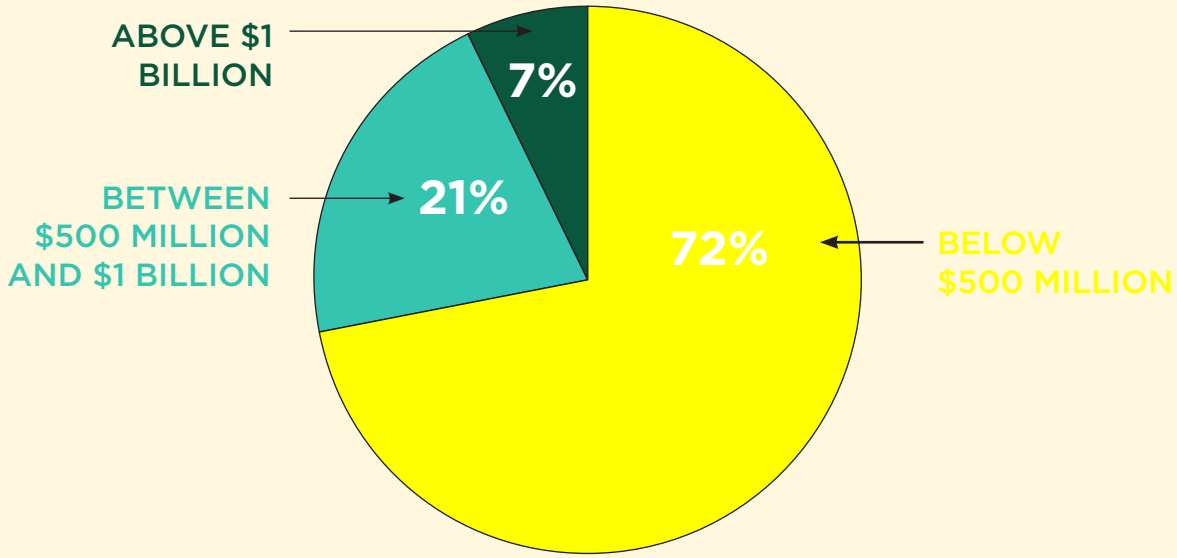
APCIA respondents offered similarly varied types of events that could be defined as catastrophic, from critical infrastructure attacks to a widespread data breach.

SURVEY PARTICIPANTS

APCIA respondents to the anonymized survey had varying business models and cyber policy writings. There was a cross-section of admitted and non-admitted cyber insurers and reinsurers among APCIA respondents.

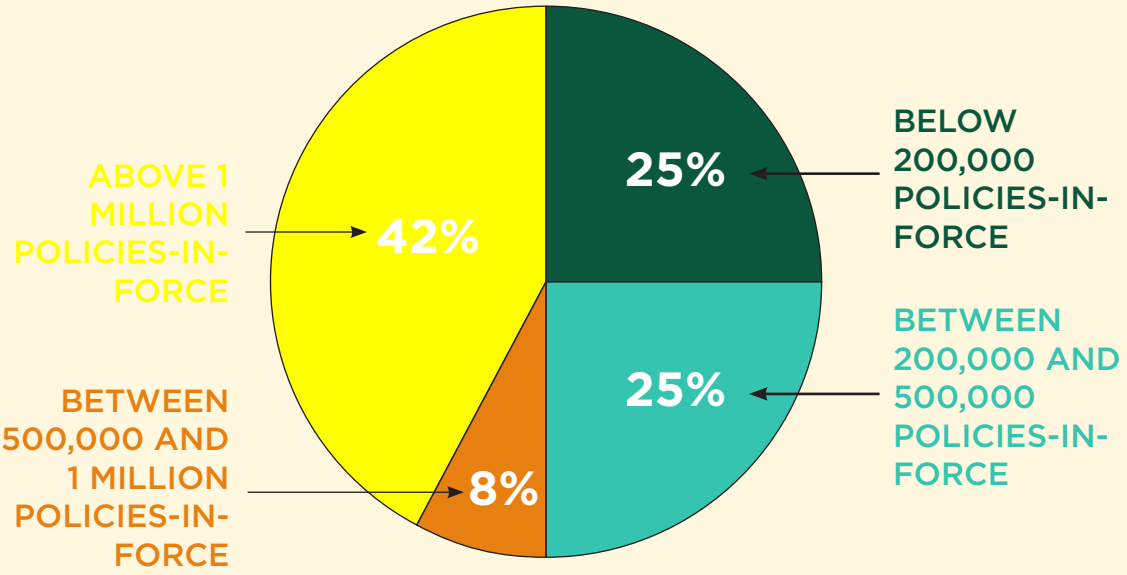


The range of cyber insurance premiums written in 2023 by APCIA respondents was as follows:

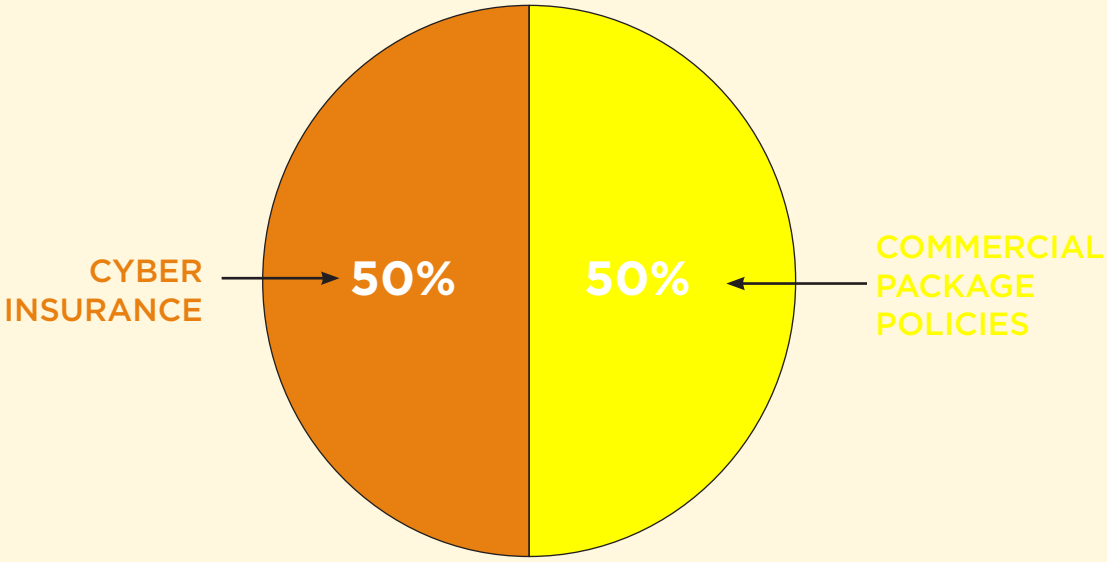


SURVEY PARTICIPANTS CONTINUED

Companies with varying policies-in-force volumes for all lines of business were represented among APCIA respondents:

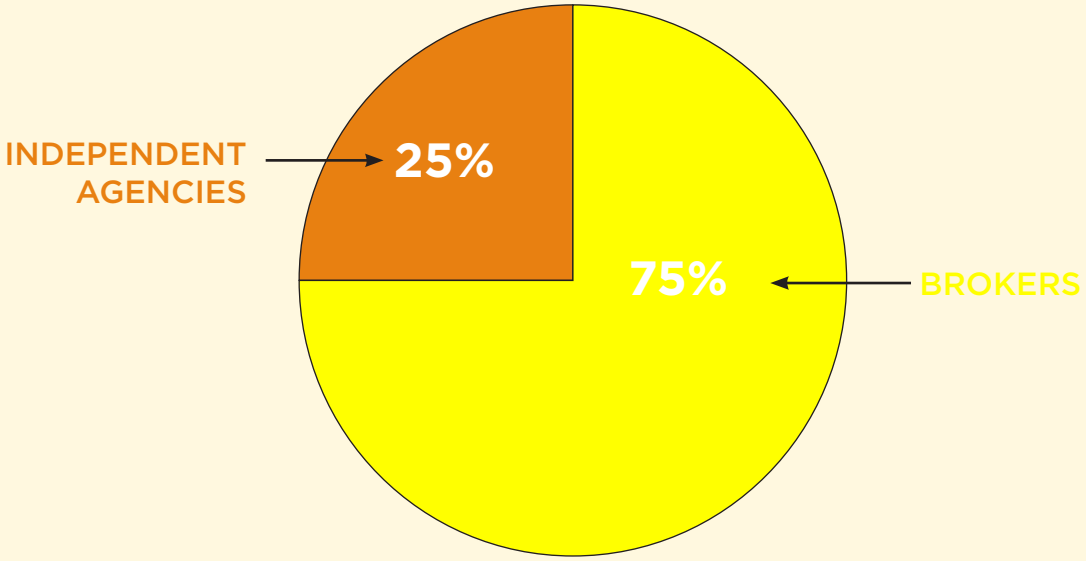


APCIA respondents' estimated policies-in-force were evenly split between stand-alone cyber insurance (50%) and commercial package policies (50%).



SURVEY PARTICIPANTS CONTINUED

Council respondents identified as brokers (75%) and independent agencies (25%), and varied in the types of cyber policies they place.



Roughly **67%** said the typical cyber insurance policy limit was **$1 million,** with a few respondents citing **$2 million, $5 million,** and **$20 million.** Most respondents' largest limit placed ranged from **$10 million** to **$30 million**, with the largest identified at **$450 million**. In the past year, the typical claim has varied from **$20,000** to over **$1 million**, with the average size ranging from **$50,000** to **$350,000**, according to Council respondents.

DETAILED INSIGHTS

MARKETPLACE GAPS IN AVAILABLE CYBER COVERAGE

APCIA respondents identified certain marketplace gaps for first-party cyber insurance coverage relating to the amount of insurance that can be purchased and applicable waiting periods. For example, insurers offer many coverages on a sublimited basis (contingent business interruption, social engineering, etc.) or subject to a waiting period. However, some insureds want business interruption coverage to apply at minute one of the disruption, which may not be available in the marketplace.

Most Council respondents affirmed that marketplace gaps exist for both first-party and third-party coverages. They identified indemnity payments, incident response services, and social engineering/invoice manipulations as the gaps in first-party coverage. APCIA respondents also identified cyber-crime coverage (social engineering/financial funds transfer) as a potential marketplace gap, though some carriers offer this coverage with a sublimit and the coverage may also be provided by crime insurance.

Both APCIA and Council respondents identified security breach liability coverage as a third-party marketplace gap.

APCIA respondents noted that commercial cyber insurance policies generally exclude coverage for events/losses resulting from (cyber) war and non-availability of critical infrastructure services, notably the electric grid or internet. Other exclusions may include nuclear events or natural catastrophes.

> *... commercial cyber insurance policies generally exclude coverage for events/losses...*

Some business' coverage needs may not be available in the market. APCIA respondents highlighted cyber-related physical damage and acts sponsored by nation-states as the most common marketplace gaps. Other potential gaps include coverage-limit inadequacy, and a lack of incident response services including non-breach regulatory compliance costs and fines, along with other contractual penalties.

Similarly, Council respondents noted that commercial clients are seeking first- and third-party coverage with adequate limits, acts of state-sponsored terrorism, cyber-related physical damage, and incident response service.

Some larger insureds in certain industry classes are seeking to in-fill the waiting period for business interruption coverage.

When asked if any of the marketplace gaps identified could be addressed in the short-term (three years of fewer), over half of APCIA survey respondents believe the insurance market will be able to fill in the gaps. Council respondents indicated the same.

The first- and third-party marketplace gaps expected to be met in the short-term included incident response services, indemnity payments, coverage limit inadequacy, incident response services, and security breach liability coverage.

Cyber insurers are continuously developing new forms of language and manuscript wordings to address competitive market needs.

Seventy-five percent of APCIA respondents believe most identified cyber insurance market gaps would be addressed in the long-term.

RISK SELECTION GAPS

Both sets of survey respondents understand that it may be difficult to obtain coverage for certain risk types in the cyber insurance market, including government entities, utilities, and education including higher education institutions.

The challenge of securing cyber insurance could also extend to high-hazard risk classes such as critical infrastructure, energy, manufacturing, healthcare, logistics, and transportation including airlines.

Cyber insurers are helping clients understand that minimum cybersecurity practices are needed to insure businesses obtain the coverage they want.

CONSIDERATIONS IN DEFINING CATASTROPHIC CYBER EVENTS

APCIA and Council respondents were asked to consider three different categories in terms of what could be defined as a catastrophic cyber event: industries impacted, a potential dollar threshold, and the nature of the event.

APCIA respondents indicated that a catastrophic cybersecurity event may be caused by outages of critical infrastructure services, such as banking, telecom, or logistics. Financial consequences due to cyber-induced outages of such services may not be covered under a cyber insurance policy. While these events may be covered under policies issued to the individual service provider being targeted, cascading losses from disruptions to energy or telecom services may not be covered. These scenarios also present a notable loss potential and are largely linked to incidents involving specific critical industries.

... a catastrophic cybersecurity event may be caused by outages of critical infrastructure services, such as banking, telecom, or logistics.

The types of events that were identified as potential catastrophic cyber events varied but included widespread critical infrastructure attacks which spread out to multiple dependencies, infrastructure outage (non-cloud), cloud outage, self-propagating malware, zero- day vulnerability exploitation, supply chain injected into legitimate software, and a widespread data breach.

A catastrophic cybersecurity event may also be caused by (cyber) war, terror, natural catastrophes, or nuclear events.

American Property Casualty Insurance Association℠
INSURING AMERICA apci.org

THE COUNCIL
The Council of Insurance Agents & Brokers

ABOUT APCIA

The American Property Casualty Insurance Association (APCIA) is the primary national trade association for home, auto, and business insurers. Our mission is to promote and protect the viability of private competition for the benefit of consumers and insurers. Our members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and internationally.
https://www.apci.org

ABOUT THE COUNCIL

The Council of Insurance Agents & Brokers (CIAB) is the premier association for the leading commercial insurance and employee benefits intermediaries around the world. Our membership annually places 85 percent of U.S. property/casualty insurance premiums and comprises the fastest growing, most innovative firms in the industry, with more than 20 percent headquartered internationally.
https://www.ciab.org

APCIA CONTACTS:

Gary Sullivan
Senior Director, Emerging Risks
American Property Casualty Insurance Association
Gary.Sullivan@apci.org

Kristin Abbott
Senior Director and Counsel, Cyber & Privacy
American Property Casualty Insurance Association
Kristin.Abbott@apci.org

THE COUNCIL CONTACT:

Nicole Vasile
Vice President of Marketing and Communications
The Council of Insurance Agents & Brokers
Nicole.Vasile@ciab.com