United States Government Accountability Office

Report to Congressional Committees

May 2021

CYBER INSURANCE

Insurers and Policyholders Face Challenges in an Evolving Market

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-477

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.

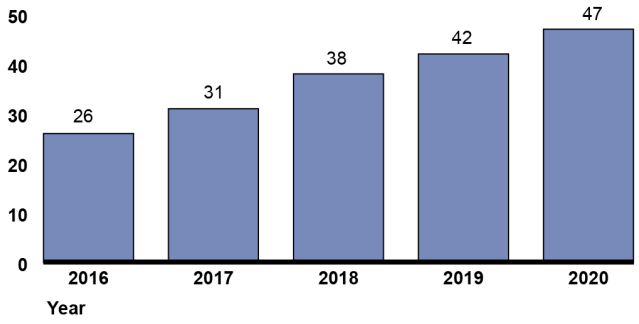
View GAO-21-477. For more information, contact John Pendleton at (202) 512-8678 or pendletonj@gao.gov.

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.

Contents

Figures

Abbreviations

NAIC	National Association of Insurance Commissioners
Treasury	Department of the Treasury
TRIA	Terrorism Risk Insurance Act
TRIP	Terrorism Risk Insurance Program

441 G St. N.W.
Washington, DC 20548

May 20, 2021

The Honorable Jack Reed
Chairman
The Honorable James M. Inhofe
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Armed Services
House of Representatives

The cost of malicious cyber activity to the U.S. economy was between $57 billion and $109 billion in 2016, according to the White House Council of Economic Advisers.[1] Since 1997, we have designated cybersecurity as a government-wide high-risk area, and U.S. businesses and other entities continue to face significant cybersecurity risks with the potential for large losses.[2] Some members of Congress and others have raised questions about the availability, affordability, and stability of the cyber insurance market. Cyber insurance is a broad term for policies that cover liability and property losses from events adversely affecting electronic activities and systems.[3]

The National Defense Authorization Act for Fiscal Year 2021 includes a provision for us to review the state and availability of insurance coverage in the United States for cybersecurity risks.[4] This report addresses (1) the

[1]Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy* (Washington, D.C.: February 2018).

[2]GAO, *High Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C: Mar. 2, 2021).

[3]More specifically, cyber insurance generally refers to policies that address first-party losses to a policyholder and third-party losses to a policyholder's client or customer as a result of an event that jeopardizes the confidentiality, integrity, and availability of an information system.

[4]William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 9005, 134 Stat. 3388, 4777 (2021).

state of coverage and key trends in the current market for cyber insurance, and (2) identified challenges faced by the cyber insurance market and potential options to address them. The focus of this report is cyber insurance provided to businesses and other entities and not to individual consumers.

To describe the current market for cyber insurance, we reviewed publicly available data from the National Association of Insurance Commissioners (NAIC), including on premiums and policies in force. We evaluated the reliability of the data by comparing NAIC's reported aggregate figures for domestic insurers to a S&P Global Market Intelligence database of cyber supplement data submitted by individual domestic insurers, and assessed NAIC's methods for estimating premiums when they were not reported.[5] We also determined what cyber coverage might not be reported, evaluated premium and policy data on surplus line insurers domiciled outside the United States, interviewed staff from NAIC and industry stakeholders, and performed electronic tests. We found the data, after adjustment to the 2016 estimate of nonreported package policy premiums, sufficiently reliable for reporting aggregate market trends. We also reviewed data on take-up rates (the proportion of entities electing coverage) from Marsh McLennan, a global insurance broker and risk-management firm. We reviewed reports from the Department of the Treasury (Treasury) and NAIC on the markets for cyber insurance and terrorism risk insurance. We interviewed industry participants and reviewed industry market reports, including from Marsh McLennan; A.M. Best, a global credit rating agency specializing in the insurance industry; the Council of Insurance Agents and Brokers, an association of large commercial insurance and employee benefits brokerages; and the Insurance Information Institute, an online provider of insurance information to consumers. We also interviewed staff from Treasury and NAIC.

To identify key challenges the market faces and potential options to address them, we reviewed reports and statements from federal and state officials, including Treasury, NAIC, the Department of Homeland Security's insurance industry working sessions, and the U.S.

[5]In 2015, state insurance regulators, through NAIC, developed the Cybersecurity and Identity Theft Coverage Supplement for insurers' annual financial statements, which requires insurers providing this coverage to report to NAIC data including policies in force, premiums, claims, and losses.

Cybersecurity Solarium Commission.[6] We also reviewed reports and statements and interviewed industry participants to obtain their perspectives on challenges in the market and options for addressing them. These industry participants included Marsh McLennan and A.M. Best, two industry associations that represent cyber insurance providers, a company that provides insurers with sample policy forms and standardized policy language, and one large cyber insurance provider.[7] We also reviewed reports from researchers and academics, including from an international think tank, an independent nongovernmental organization, and a professional organization representing actuaries. The information we obtained from these industry participants and researchers may not represent the views and practices of all industry participants or researchers.

We conducted this performance audit from January 2021 to May 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

A cyber incident is defined as a cyber event that jeopardizes the cybersecurity of an information system or the information the system processes, stores, or transmits; or an event that violates security policies, procedures, or acceptable use policies, whether resulting from malicious activity or not.[8] Cyber incidents, including cyberattacks, can damage information technology assets, create losses related to business disruption and theft, release sensitive information, and expose entities to liability from customers, suppliers, employees, and shareholders.

[6]U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, D.C.: March 2020). The commission is a bipartisan, intergovernmental body, created by statute to develop a strategic approach to defense against significant U.S. cyberattacks. Department of Homeland Security, National Protection and Programs Directorate, *Insurance Industry Working Session Readout Report: Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues* (Washington, D.C.: July 2014).

[7]The industry associations were the Council for Insurance Agents and Brokers and American Property Casualty Insurance Association.

[8]Financial Stability Board, *Cyber Lexicon* (Nov. 12, 2018).

Some private insurance companies offer businesses and other entities cyber insurance to protect against first-party (policyholder) and third-party losses (policyholder's clients or customers) from an event that jeopardizes the confidentiality, integrity, and availability of an information system. The insurance can be provided through a standalone policy that provides only cyber insurance coverage or as a part of a package policy that provides multiple types of coverage, such as a general commercial liability insurance policy.

States regulate the private insurance market, including for cyber insurance. The regulators seek to ensure that insurance policy provisions comply with state law, are reasonable and fair, and do not contain major gaps in coverage that might be misunderstood by consumers and leave them unprotected. States generally do not establish minimum standards for cyber insurance policy coverage; they largely have focused on the solvency of cyber insurers, according to NAIC.[9] Some states and NAIC have promoted cybersecurity and data protections for insurers.[10]

The Federal Insurance Office in Treasury administers the Terrorism Risk Insurance Program (TRIP), which requires the federal government to share some losses with private insurers in the event of a certified act of terrorism. Losses from cyberattacks might be reimbursed under TRIP if the attacks met certain certification criteria specified by the program. We will be issuing a report later in 2021 that examines (1) the risks and costs of cyberattacks on U.S. critical infrastructure; (2) insurance coverage that is available for losses related to cyber risk, including cyberterrorism; and (3) the extent to which TRIP, under the Terrorism Risk Insurance Act (TRIA), is structured to respond to cyberattacks and cyberterrorism.

[9]In February 2021, the State of New York issued a Cyber Insurance Risk Framework that directs insurers to take steps to improve and enhance their cybersecurity strategy to include educating policyholders about cybersecurity and reducing the risk of cyber incidents.

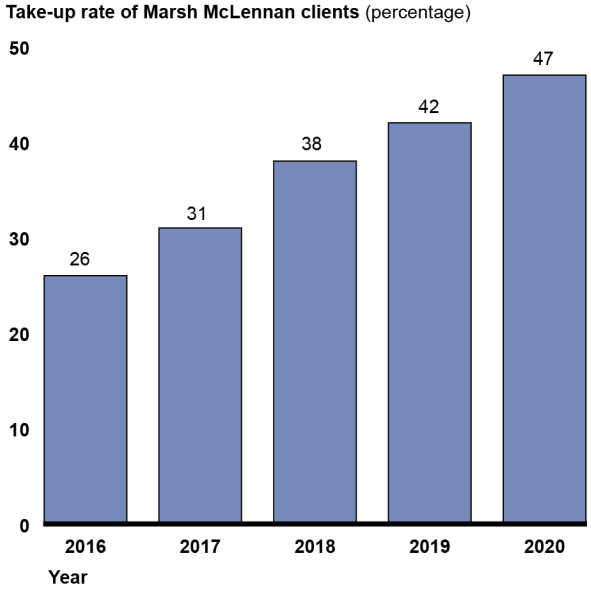
[10]In 2017, NAIC adopted the Insurance Data Security Model Law to update state insurance regulatory requirements relating to data security, investigations of cyber events, and notification to state insurance commissioners of cybersecurity events at regulated entities.

Cyber Insurance Coverage Varies by Industry and Entity Size, but Growing Cyber Risk Creates Uncertainty in Evolving Market

Cyber Coverage Varies by Industry and Entity Size

One way of assessing the extent of coverage among businesses is through take-up rates. Insurance take-up rates refer to the percentage of entities eligible for coverage that elect to take it. According to Marsh McLennan, its clients' cyber insurance take-up rates rose from 26 percent in 2016 to 47 percent in 2020 (see fig. 1).[11]

Figure 1: 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

[11]Marsh McLennan is the largest commercial insurance broker of U.S. business, by revenues, according to the Insurance Information Institute's 2021 Insurance Fact Book.

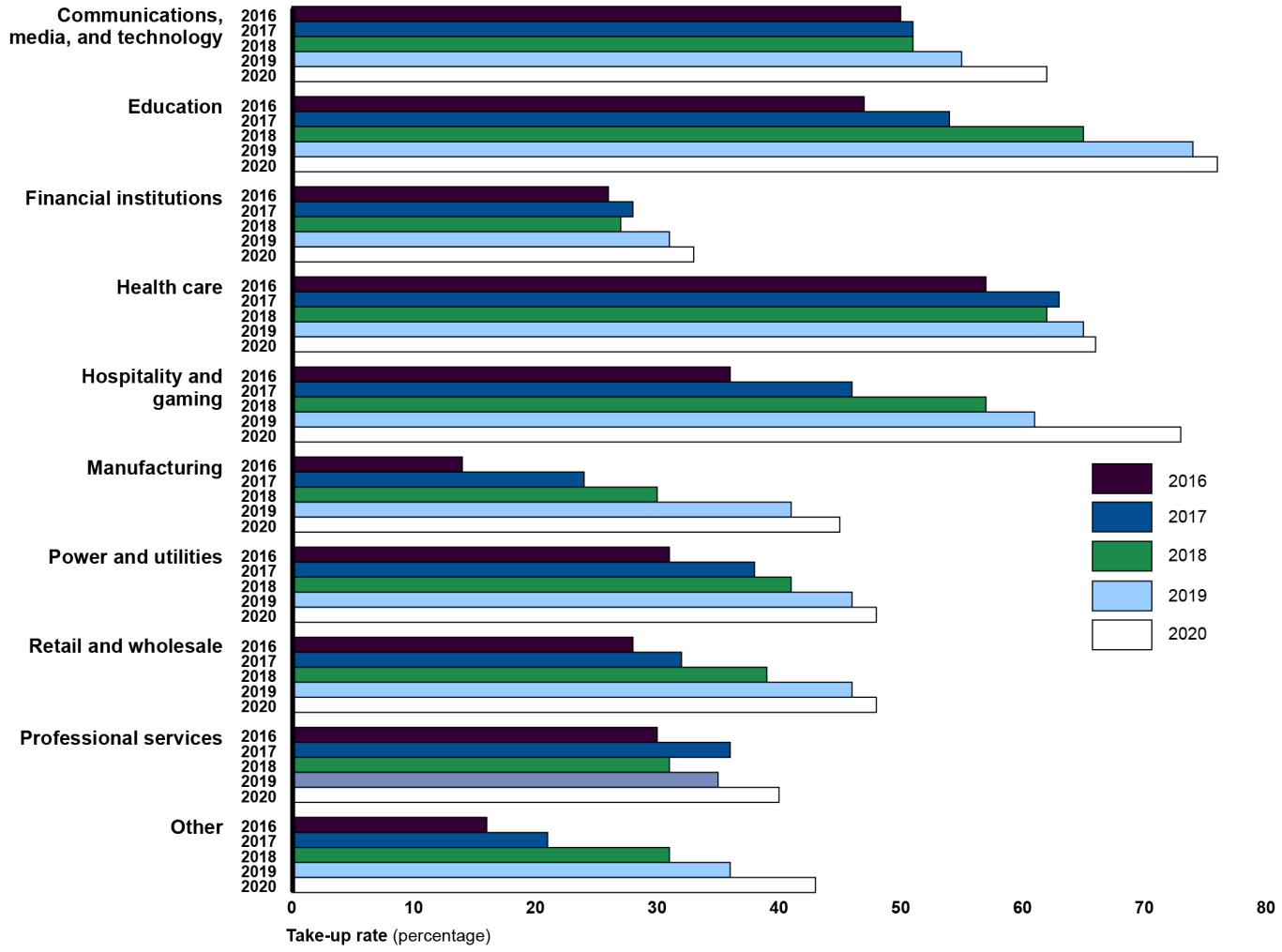
Note: Insurance take-up rate refers to the percentage of entities eligible for coverage that elect to take it. These figures represent take-up rates of Marsh McLennan clients that used Marsh McLennan as their broker to obtain cyber coverage. Take-up rates for Marsh McLennan clients overall may be higher because some clients may use another broker to obtain coverage.

Industry sources, including Marsh McLennan, also have reported that take-up rates for small and mid-size entities lag those of larger entities.[12] According to industry representatives and reports, a combination of factors likely contributed to lower take-up rates for small and mid-size entities: underestimation of cyber risks, difficulty understanding coverages, belief that current coverage is adequate, and affordability concerns.

Take-up rates also vary by industry. According to Marsh McLennan, among its clients, the industry sectors with the highest take-up rates in 2016–2020 included education and health care, which collect, maintain, and use significant amounts of personally identifiable information or protected health information (see fig. 2). Sectors experiencing significant growth in take-up in that period included the hospitality and retail sectors, which commonly collect payment card information. The manufacturing sector's take-up rate also grew significantly, as that industry became increasingly aware of potential cyberattack risks, according to industry sources.

[12]No uniform standard exists for defining the size of an entity for insurance purposes, although number of employees and annual revenue are frequently used as proxies. For example, the Insurance Information Institute notes that small businesses are typically those with fewer than 50 employees, although common small business policies are available for businesses with fewer than 100 employees. According to Marsh McLennan, entities with revenues of $250 million or less are generally considered part of the small and mid-size market and businesses with revenue up to $1 billion are generally considered mid-size. The Insurance Information Institute also generally considers businesses with 50–1,000 employees and revenues from $10 million to $1 billion to be mid-size.

Figure 2: Cyber Insurance Take-up Rates for a Selected Large Broker's Clients, by Industry, 2016–2020



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

Note: Insurance take-up rate refers to the percentage of entities eligible for coverage that elect to take it. Figures do not include Marsh McLennan clients that did not also use the company as their insurance broker to obtain cyber coverage.

Various industry sources described their opinions on the availability and affordability of cyber insurance. The Council of Insurance Agents and Brokers told us coverage has been available and affordable since at least 2016 for the majority of entities of various sizes and across industries. NAIC officials agreed that cyber insurance is generally currently available and affordable, but noted this varies based on business size. Small businesses may purchase cyber insurance less often if they perceive their risks to be minimal or policies too costly. Representatives from the

Insurance Information Institute identified several factors such as industry type and a business's use of data that may affect the cost and affordability of coverage.

The extent to which cyber insurance will continue to be generally available and affordable remains uncertain. Despite the upward trend in take-up rates to date, insurer appetite and capacity for underwriting cyber risk has contracted more recently, especially in certain high-risk industry sectors such as health care and education and for public-sector entities, according to the Council of Insurance Agents and Brokers, Marsh McLennan, and A.M. Best.[13] These sources noted the contraction has resulted from factors that include increasing losses from cyberattacks, the threat of future attacks, and overall insurance market conditions.

According to industry representatives and reports, underwriters have been more carefully scrutinizing the risks posed by all entities, regardless of size or sector, which could affect future cyber insurance availability and affordability. They noted that insurers have become more selective in extending coverage to high-risk entities and industries and increasing prices of coverage they offer. This caution has been in response to the increasing frequency, severity, and cost of cyberattacks and uncertainty about the type, scope, and targets of future attacks.

Growing Risks Have Created Uncertainty in Evolving Cyber Insurance Market

Recent trends in the cyber insurance market include increasing demand, higher premiums, a growing number of industry participants, and more restrictive policy terms and coverage limits.

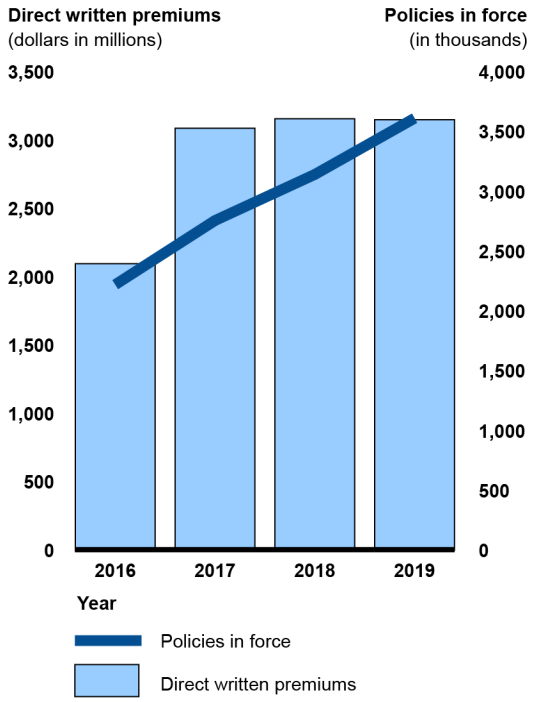
Increasing demand. The demand for cyber insurance has increased as entities better understand and respond to increasing cyber risks. According to our analysis of data from S&P Market Intelligence and NAIC, the number of cyber insurance policies in force increased by about 60 percent in 2016–2019, from about 2.2 million policies to more than 3.6 million policies (see fig. 3).[14] The amount of total direct written premiums

[13]Capacity is the maximum amount of insurance an insurer can underwrite and remain financially solvent.

[14]Policies in force are those that are active and for which premiums have been paid or are being paid.

increased by about 50 percent during this period, from $2.1 billion to $3.1 billion.[15]

Figure 3: Direct Written Premiums and Policies in Force for Cyber Insurance, 2016–2019



Source: GAO analysis of S&P Market Intelligence and National Association of Insurance Commissioners data. | GAO-21-477

Note: Data include standalone and package cyber insurance premiums and policies in force reported by both U.S. domiciled insurers and non-U.S. surplus lines insurers and reflect estimates for unreported amounts. As of April 2021, complete data for 2020 were not available. The completeness, consistency, and comparability of data may be limited due to insurers' difficulty estimating premiums for cyber coverage included in package policies with other property and liability coverages. Direct written premiums for 2016 reflect GAO adjustments to NAIC's estimate of package policy premiums not reported by insurers.

According to one industry survey, more than 60 percent of brokers surveyed reported that the top two drivers of new or increased sales of cyber insurance were clients experiencing a cyberattack or hearing that

[15]Direct written premiums are the dollar value of premiums an insurer receives on a policy without any adjustment for any portion of premiums ceded to reinsurers. Because insurers record written premiums as of the effective date of a policy contract, the recorded amount may include premiums earned in a different period.

others suffered losses from an attack.[16] Another survey noted that that 75 percent of responding agents and brokers reported an increase in demand for cyber coverage in the fourth quarter of 2020.[17]

Higher premiums. After holding relatively steady in 2017 and 2018, cyber insurance premiums increased markedly in 2020, as shown in figure 4. Moreover, more than half of brokers recently surveyed reported that their clients experienced a 10–30 percent price increase in cyber insurance premiums from the third to the fourth quarter of 2020. Only 15 percent of these brokers reported no change in premium price during this period.[18] Higher prices for cyber insurance have coincided with increased demand for the product and higher insurer losses from increasingly frequent and severe cyberattacks (particularly ransomware attacks that block users from accessing systems or data until a ransom is paid), according to A.M. Best, the Council of Insurance Agents and Brokers, and NAIC.[19]

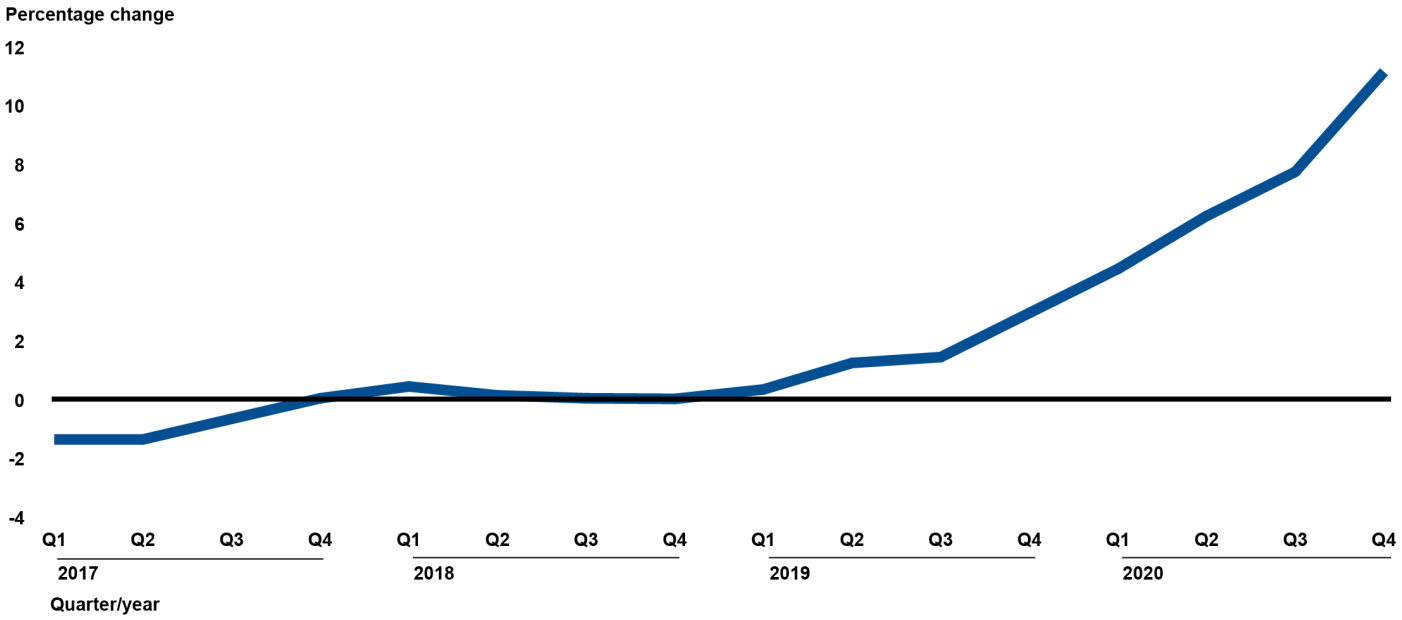
[16]Advisen and PartnerRe, *Cyber Insurance–The Market's View* (September 2020).

[17]The Council of Insurance Agents & Brokers, *Commercial Property/Casualty Market Index, Q4/2020* (Washington, D.C.: Feb. 17, 2021).

[18]Commercial Property/Casualty Market Index, Q4/2020.

[19]Losses and related claims defense costs paid as a percent of direct written premiums (direct loss and loss cost ratio) rose from 16 percent in 2016 to 33 percent in 2019 for standalone cyber policies. Fitch Ratings stated that it believes that cyber underwriting performance will continue to deteriorate as underwriting exposure grows, coverage broadens, and the nature of cyber claims evolves.

Figure 4: Change in Cyber Insurance Premiums, 2017–2020



Source: GAO presentation of data from Council of Insurance Agents & Brokers. | GAO-21-477

Factors that can affect the extent of premium increases include the size of a company, its industry, and the extent to which it has strong cyber controls. For example, brokers specializing in cyber insurance for small and mid-size entities told us that average premiums for cyber policies currently range from about $1,400 to about $3,000 per million of limit for small entities that have strong cyber controls and are in low-risk industries. Premiums can be many times that amount depending on entity and industry risk factors.[20] These same brokers told us premium increases in 2021 were expected to be larger for high-risk industries and mid-size and larger entities than for smaller entities, where premium

[20]One broker told us that minimum premiums for high-risk industries with revenues up to $5 million can range from $2,000 to $3,500 per million of limit, while other brokers said premiums on policies that target mid-size entities with revenues from less than $100 million to $250 million can average from about $5,000 to more than $10,000 per million of limit. In addition to entity and industry risk factors, premiums can differ based on the amount of a deductible or other self-insured amount, which the brokers told us had minimums from $1,000 to $5,000 for policies with a $1 million total limit. These same risk factors also can result in lower coverage limits for certain perils, such as $250,000 for social engineering and wire transfer attacks on a policy with a $1 million total limit.

increases are expected by one broker to be more in the range of 5–10 percent for those with strong cyber controls.

More industry participants in a concentrated market. The number of insurers offering cyber coverage increased by about 35 percent between 2016 and 2019, according to our analysis of NAIC's cyber supplement data. However, new market participants (insurers entering the cyber market after 2016) represented only about 9 percent of total premiums written in 2019. The cyber insurance market is more concentrated than the property and casualty insurance market as a whole. Our analysis of S&P Market Intelligence Market Share Report and cyber supplement data showed that 10 U.S. insurance groups wrote nearly 70 percent of cyber insurance premiums in 2019, but represented 18 percent of total property and casualty insurance premiums in 2019.

More cyber-specific policies. Insurers offer affirmative cyber coverage—that is, coverage specific to cyber risk. This insurance is offered through standalone cyber policies, package policies that combine cyber coverage with professional liability coverages, and, less frequently, through an affirmative cyber endorsement to other lines of coverage.[21] Industry sources have noted that the increase in cyber-specific policies may reflect a desire for coverage of losses related to the confidentiality, integrity or availability of data and systems and clarity about what is covered, which in turn may help reduce claims disputes and litigation in the event of a cyberattack. Standalone policies also provide policyholders with a greater potential for higher cyber-specific limits.[22]

Reduced coverage limits for certain sectors. According to industry representatives and reports, the continually increasing frequency and severity of cyberattacks, especially ransomware attacks, have led insurers to reduce cyber coverage limits for certain riskier industry

[21]Standalone policies cover specific types of risk, such as cyber risk. Other property and casualty policies, such as those for commercial multi-peril, offer broad coverage for a number of risks. Package policies combine property and liability coverages (such as by adding an endorsement for cyber risk) into a single insurance contract.

[22]Almost 60 percent of brokers responding to a recent industry survey stated their clients sought to switch from an endorsement to a standalone policy to obtain a dedicated limit, while almost 40 percent said the motivation to switch was a desire to obtain a higher limit offered through a standalone policy. *Cyber Insurance–The Market's View*.

sectors, such as health care and education, and for public entities and to add specific limits on ransomware coverage.

Tighter terms and more exclusions. Industry participants have noted that insurers have been tightening policy terms and conditions for cyber-specific policies. They also have been adding exclusions to traditional lines of coverage and package policies with cyber endorsements to avoid any ambiguity that coverages would overlap with cyber policies. These restrictions seek to eliminate coverage of "silent" cyber risks that could damage multiple businesses and result in insurers accumulating significant unforeseen losses that could pose a risk to their solvency.[23] A.M. Best representatives said that "silent" cyber is unlikely to be eliminated in the short term, but continued movement towards standalone cyber and clarification of policy language could help.

Cyber Insurance Industry Faces Multiple Challenges, but Options Have Been Proposed to Address Them

Key challenges facing the cyber insurance market include data limitations, limited awareness of cybersecurity risks by businesses, and the risk of aggregated losses from a cyberattack, according to insurers, brokers, and other industry members we interviewed and literature we reviewed. Several potential options have been proposed for federal and state governments and the insurance industry to address some of these challenges.

Limited Historical Data Exist on Cyber Losses and Events

One challenge facing the cyber insurance industry is limited availability of historical loss and cyber event data, according to industry reports and experts we interviewed. Insurance companies use historical loss data to quantify risk and set premium rates for insurance products. However, according to reports by industry participants and a government entity, historical data on cyber losses are very limited, incomplete, or of poor quality.[24] According to a report by the Deloitte Center for Financial Services, these limitations make it difficult to build the predictive models

[23]Silent risk refers to coverage that is not explicitly granted or excluded in insurance policies ("non-affirmative" risk).

[24]Reasons for data limitations include the relative newness of the cyber insurance market, the fact that most cyberattacks go unreported or undetected, and the lack of a centralized source for information about cyber events.

that help assess the probability of loss from a cyberattack. [25] That report also noted no comprehensive, centralized source of information about cyber events exists for insurers to access.[26] In addition, a 2020 report by the International Association of Insurance Supervisors noted that incomplete or inaccurate historical data on cyber incidents decreases the reliability of actuarial models, leading to increases in uncertainty around loss estimates.[27] Without access to such data, some industry participants and researchers are concerned that current prices for cyber policies may not accurately reflect risk. According to NAIC, if a product is priced too low, an insurer may not have the financial means to pay claims to the policyholder, which could lead to insolvency. If priced too high, few businesses and consumers might be able to afford the coverage.

Opportunities exist for improving the nation's capacity for collecting cyber event and loss data and for coordinating industry-wide efforts to collect and share that information. According to a recent report by the U.S. Cyberspace Solarium Commission, Congress could establish an entity to collect data to better understand cyber risk and help the insurance industry create better risk models.[28] The commission also suggested that a public-private working group could be established at the Department of

[25]Deloitte Center for Financial Services, *Demystifying Cyber Insurance Coverage: Clearing Obstacles in a Problematic but Promising Growth Market* (Deloitte University Press, 2017).

[26]Historical loss data are used to build predictive models about expected costs, which are part of the ratemaking process. These models are partly based on what the estimated loss will be from specific events, such as data breaches or ransomware attacks. According to Marsh McLennan, because there is no precedent for insurable cyber catastrophic events, the insurance industry has drawn parallels or made assumptions based on lessons learned from other lines of business and "near misses" in the cyber line of business, or both. Deloitte and the U.S. Cyberspace Solarium Commission suggest that access to data on cyber events would facilitate decision-making for insurers as it relates to modeling and pricing.

[27]International Association of Insurance Supervisors, *Cyber Risk Underwriting: Identified Challenges and Supervisory Considerations for Sustainable Market Development* (Basel, Switzerland: December 2020).

[28]The commission's report also includes recommendations to enact a national cyber incident reporting law requiring critical infrastructure agencies to report cyber incidents to the federal government, where the data would be anonymized and shared with a new entity charged with collecting and providing cybersecurity data to inform policymaking and government programs. The report recommends that the data entity act as a statistical agency that collects, processes, analyzes, and disseminates essential data on cybersecurity and cyber incidents to the public, Congress, federal agencies, state and local government, and the private sector.

Homeland Security to convene insurance companies and cyber risk modeling companies to collaborate on pooling available data that could inform innovations in cyber risk modelling.

Support for better data collection dates back several years. During Department of Homeland Security working sessions of the Cyber Incident Data and Analysis Working Group, industry participants suggested that an anonymized cyber incident data repository could foster voluntary data sharing about attacks, data breaches, and business interruptions. Participants suggested that a repository to share, store, aggregate, and analyze sensitive cyber event data would help promote greater understanding of the financial and operational effects of cyber events.[29]

Cyber Policies Lack Common Definitions

Our review of several reports on the industry by a U.S. agency and researchers indicates that terms commonly used in cyber policies are not consistently defined. Representatives from the Insurance Services Office, a company that has produced widely used sample policy forms and standardized policy language, said that the language used in cyber policies with more than $5 million in coverage varies greatly.[30] They noted that carriers may use slightly different language in their definitions. A report by the Congressional Research Service found a lack of consensus on what defines a cyberattack.[31] Similarly, a report by the Geneva Association noted that neither “cyber war” nor “cyberterrorism” have a

[29]On May 12, 2021, the president issued an Executive Order on cybersecurity that directs federal contractors providing technology services to share information and data related to cyber threats and incidents with the Cybersecurity and Infrastructure Security Agency (CISA) and agencies with which they have contracted. The Executive Order further directs CISA to centrally collect and manage this information. As part of the implementation of this order, the Secretary of Defense acting through the Director of the National Security Agency, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence is directed to develop procedures for ensuring that cyber incident reports are promptly and appropriately shared among agencies. Executive Order on Improving the Nation’s Cybersecurity (May 12, 2021).

[30]The Insurance Services Office representatives told us they have noticed that policies with more than $5 million in coverage are typically more specialized and customized to each client.

[31]Congressional Research Service, *Cyberwarfare and Cyberterrorism: In Brief*, R43955 (Washington, D.C.: Mar. 27, 2015).

common definition in the insurance market.[32] It also noted that no global consensus exists on the exact behavior or criteria that define a cyber event as either terrorism or warfare.[33] Finally, representatives from the Council of Insurance Agents and Brokers told us insurers may define ransomware attacks in different ways.

Staff from NAIC also told us that inconsistent policy language, which includes the definition of key policy terms, might present challenges for the insurance industry. They explained that if the industry does not use consistent definitions for key policy terms, it will not be clear which perils are covered and which are excluded, making it difficult to move toward greater policy standardization.[34] In addition, this ambiguity can result in misunderstandings and litigation between insurers and policyholders.[35]

According to the Geneva Association, common terminology could lead to a more sustainable cyber market in which insurers could make informed choices about the levels of coverage and policyholders could understand their insurance protection. Some industry stakeholders recommended increased clarity and transparency in insurance language, including uniform definitions for key insurance terms.

[32]The Geneva Association is an international organization that conducts research in different areas of the insurance industry, including cyber. The Geneva Association reported that the definitions and understanding of cyberterrorism and cyberwarfare may differ depending on the way they are applied in different settings, such as military or political. The use of these insurance terms has varied between jurisdictions, companies, and lines of business. The Geneva Association, *Cyber War and Terrorism: Towards a common language to promote insurability* (July 2020).

[33]The Geneva Association introduced "hostile cyber activity" as a potential term for the insurance industry to mitigate the ambiguity surrounding policy wording in the context of war and terrorism.

[34]The Council of Insurance Agents and Brokers also stated that it is challenging to determine which events are considered "cyberterrorism" because this is not an official industry term.

[35]In June 2017, Russian cyber operators launched destructive malware adapted from vulnerabilities common to unpatched Windows operating systems, which quickly spread worldwide. The NotPetya attack exposed some of the ambiguities in policy treatment of certain cyber incidents. Several companies affected by this attack filed multiple claims with their property and casualty insurers. Some of the insurers paid out the NotPetya claims and others denied the claims by invoking a "war exclusion," which is common in some policies but had not been applied to cyber incidents. The companies sued the insurance companies that denied the claim and the case remains in litigation.

Some Businesses Have Limited Awareness of Cyber Risks and Coverage

Several industry associations, regulators, and participants said that many entities, particularly smaller businesses, may underestimate their cyber risks and the cyber coverage needed to mitigate those risks. According to Marsh McLennan, insurance with inadequate limits and insufficient coverage can lead to protection gaps, which increases a company's financial exposure.[36] According to the Geneva Association, the annual global economic cost of cyber incidents may be almost twice the average annual amount of natural disaster losses. A survey by the Better Business Bureau found 87 percent of small business respondents believed they were vulnerable to cyberattacks.[37] However, industry participants and a regulator have stated that smaller entities may not fully appreciate the magnitude of the cyber risk they face and the potential effects and costs to their business of a cyberattack. Reports by several industry researchers also indicate that some businesses are hesitant to purchase cyber insurance because they do not see its value, believe it will not provide for recovery from a cyberattack, or believe the coverage includes too many exclusions.[38]

The Council of Insurance Agents and Brokers has suggested that the insurance industry, including insurance agents and brokers, can help companies understand the risk, impact, and cost of a cyberattack on their operations. They also advise that customers evaluate their cyber risk and understand the coverage they purchase and its limits. NAIC representatives told us the industry may offer additional cyber services to help policyholders manage their cyber risk. But they added that some small and mid-size businesses have limited technical resources or staff with cybersecurity expertise and are not taking full advantage of these services.

[36]The Geneva Association defines insurance protection gaps as the difference between the amount of insurance that is economically beneficial and the amount of coverage actually purchased.

[37]Better Business Bureau, *2017 State of Cybersecurity among Small Businesses in North America* (Arlington, Va.: 2017).

[38]For example: Jon Bateman, *War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions*, Carnegie Endowment for International Peace Working Paper (Washington, D.C.: October 2020); and Organisation for Economic Co-operation and Development, *Enhancing the Role of Insurance in Cyber Risk Management* (2017).

Industry Stakeholders Cite Concerns about TRIA's Applicability for Cyberattacks

Some industry participants and a regulatory agency said they were unsure about the likelihood of Treasury certifying cyberattacks as acts of terrorism, because the department has never certified any event under TRIA and cyberattack characteristics may not readily meet the act's certification requirements. For Treasury to certify an act of terrorism under TRIA, the act must be violent or dangerous to human life, property, or infrastructure, generally result in losses in the United States, and be part of an effort to coerce the civilian population of the United States or affect the conduct of the U.S. government by coercion. However, cyberattacks may not be violent, or they may cause losses to computer servers located outside the United States. In addition, cyberattacks could be conducted for financial ransom, rather than to coerce the government or population of the United States. The Centers for Better Insurance noted that if TRIA were to more openly encompass cyberattacks, Congress could amend the statute to revise the certification criteria to include acts that involve losses associated with electronic data and infrastructure, extend the geographic parameters of the program beyond damage in the United States, and broaden the scope of intent underlying the cyberattack beyond coercion. However, the Insurance Information Institute suggested that expanding TRIA coverage could have implications for the insurance market and that insurers might pull back on the property and liability insurance they offer if they felt they could not assume those levels of risk.

Some industry participants also have expressed two additional concerns. First, they noted the possibility of an extremely large cyberattack, such as to the electrical grid, exceeding the TRIA cap of $100 billion, leaving losses above the cap uninsured. TRIA's coverage cap has not been adjusted since Congress passed TRIA. Second, some participants expressed concerns about the increased level of risk borne by private-sector insurers. Congressional reauthorizations of TRIA generally shifted exposure from the federal government to the private sector.[39] In a May 2020 report, Treasury's Advisory Committee on Risk Sharing Mechanisms found that because of the shift in loss exposures, TRIP may no longer be as effective a framework for insurance industry stability as it

[39]According to our analysis of Treasury data on insurer direct-earned premiums, federal losses following a terrorist event under the loss-sharing provision in effect in 2020 would be smaller than they would have been for a similar event under the loss-sharing provision in effect in 2015, across all event sizes and subsets of insurers. See GAO, *Terrorism Risk Insurance: Program Changes Have Reduced Federal Fiscal Exposure*, GAO-20-348 (Washington, D.C.: Apr. 20, 2020).

previously was, and recommended that Treasury review the potential implications of changing the cap.

Cyber Risks Are Evolving and Could Involve Aggregated Losses

Cyber risk continues to evolve as technology and the methods of cyberattack change, making it difficult for insurers to underwrite coverage. The Federal Reserve Bank of Chicago has stated that the growing sophistication and agility of threat actors has increased insurers' cyber risk exposure. Fitch has noted that underwriting cyber insurance policies is challenging as technology advances and the connectivity of digital devices to the internet or the cloud increases. Similarly, a recent study by Deloitte found existing cyber exposures continue to change and new ones arise.[40] It noted that even as insurers collect more data and hone predictive models based on prior cyber threats, the underlying exposure keeps changing. This makes it difficult to create a reliable predictive model when it is not clear what new objective, strategy, or technique cyber threat actors may deploy.

In addition, a single cyberattack could damage multiple businesses and result in significant losses. NAIC staff told us that cyberattacks have the potential for aggregated losses—that is, the possibility that many businesses may simultaneously make claims.[41] Aggregated losses could financially challenge insurers, even posing solvency risks. The Cambridge Centre for Risk Studies similarly noted that cyberattacks can spread quickly and cause aggregated losses, which according to its 2016 report, was cited by most insurers as a primary reason for not expanding their capacity to offer cyber insurance.[42]

One example of how losses can quickly aggregate is the 2017 NotPetya malware attack that originated in Russia, struck the Ukraine, and quickly spread around the world, resulting in at least $10 billion in damages. The U.S. Cybersecurity Solarium Commission reported that the malware spread from targeted Ukrainian banks, payment systems, and federal

[40]Deloitte Center for Financial Services, *Demystifying Cyber Insurance Coverage: Clearing Obstacles in a Problematic but Promising Growth Market* (2017). Cyber exposures are vulnerabilities associated with computers or network technology that create potential losses for a business.

[41]Aggregation risk refers to the fact that a single cyberattack could damage multiple businesses, span connected systems, cover wide geographies, and result in aggregated losses from the accumulation of exposures.

[42]University of Cambridge Centre for Risk Studies, *Managing Cyber Insurance Accumulation Risk* (2016).

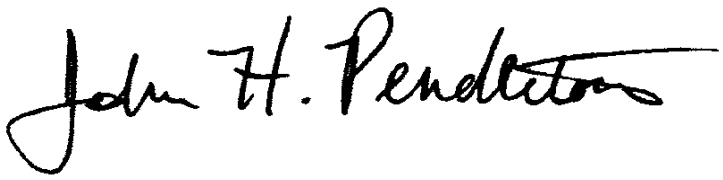
agencies to power plants, hospitals, and other life-critical systems worldwide. According to a 2020 report published by the Carnegie Endowment for International Peace, cyber risk presents a high potential for aggregated losses, and a single cyber event may result in claims from multiple sources at once.[43] Concerns about the systemic risks and potential for aggregated losses posed by such attacks have led insurers, according to Marsh McLennan, to seek loss modeling beyond that for known, non-catastrophic portfolio losses to include modeling for the impact of catastrophic cyber events. Marsh McLennan said that it expects insurers will rely more heavily on data and analytics to inform underwriting strategy, product pricing, and reinsurance purchasing as cyber portfolios continue to grow and modeling matures.

Agency Comments

We provided a draft of this report to Treasury and NAIC for review and comment. Treasury and NAIC provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of the Treasury, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-8678 or pendletonj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix I.



John H. Pendleton
Director, Financial Markets and Community Investment

[43]Jon Bateman, *War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions*.

Appendix I: GAO Contact and Staff Acknowledgments

GAO Contact

John H. Pendleton, 202-512-8678, or pendletonj@gao.gov

Staff Acknowledgments

In addition to the contact named above, Winnie Tsen (Assistant Director), Nathan Gottfried (Analyst in Charge), Evelyn Calderon, Scott McNulty, Barbara Roesmann, Stephen Ruszczyk, Jessica Sandler, Jena Sinkfield, and Andrew Stavisky made significant contributions to this report.