December 14, 2022

Attn: Richard Ifft
Senior Insurance Regulatory Policy Analyst
U.S. Department of the Treasury
Federal Insurance Office

Re: Potential Federal Insurance Response to Catastrophic Cyber Incidents
Docket ID: TREAS-DO-2022-0019-0001

On behalf of the Committee on Cyber Risk ("the Committee") of the American Academy of Actuaries,[1] we are pleased to provide comments to Federal Insurance Office (FIO) of the U.S. Department of the Treasury in response to your request for comment regarding the "Potential Federal Insurance Response to Catastrophic Cyber Incidents."

Cyber exposure and cyber insurance are of great interest to actuaries and Academy members. The Committee has compiled a number of cyber-related reports in a "Cyber Risk Toolkit." The Toolkit contains articles on topics such as: the cyber threat landscape, cyber data, risk accumulation, ransomware, cyberterrorism and war, as well as a cyber resource guide, among others. The Toolkit is a living resource in that it is updated and augmented on an ongoing basis. The Committee has also, on two occasions, (January 2021, May 2022) provided comments to Treasury regarding the functioning of the Terrorism Risk Insurance Act (TRIA) in consideration of cyber events. Finally, the Committee (in conjunction with the Academy research department) released *Cyber Breach Reporting Requirements: An Analysis of Laws Across the United States*. As the title implies, the report explores state-level requirements for data breach reporting.

Reiterating, cyber insurance is a topic upon which the Committee has spent considerable time and effort. The cyber landscape is not static, so our efforts to monitor and understand cyber exposure are ongoing.

In providing comments on cyber risk and cyber insurance, this letter addresses the following:

- Prior Academy comments on TRIA
- U.S. cyber insurance market
- Cyber catastrophes
- Cyber risk models
- Other considerations

[1] The American Academy of Actuaries is a 19,500-member professional association whose mission is to serve the public and the U.S. actuarial profession. For more than 50 years, the Academy has assisted public policymakers on all levels by providing leadership, objective expertise, and actuarial advice on risk and financial security issues. The Academy also sets qualification, practice, and professionalism standards for actuaries in the United States.

Prior Academy comments on TRIA

Since the implementation of TRIA in 2002, the frequency, severity, and the nature of cyber risks have increased significantly. The current TRIA provisions and the very nature of cyberattacks make it difficult to determine if a cyberattack will be covered under TRIA. There are several criteria that must be met for an act to be certified by the secretary of the Treasury as an act of terrorism. For an event to be certified an act of terrorism, it would have to be determined to have been:

1. committed by an individual or individuals as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States government by coercion;

2. a violent act or an act that is dangerous to human life, property, or infrastructure; and

3. have resulted in damage within the United States or in certain defined areas outside the United States.

These criteria are easily identifiable for a physical attack on United States soil, but in the case of a cyberattack, the criteria are more difficult to determine. For example, the first criterion does not apply to all cyberattacks because many are purely for financial gain (such as ransomware). Certain types of cyberattacks, such as data breaches, do not necessarily satisfy criterion two because these acts do not necessarily pose a threat to human life, property, or infrastructure. The third criterion could also be debated in a cyberattack especially when data servers are stored outside of the United States.

Systemic risk also raises challenges for the cyber insurance market including how these attacks would relate to losses covered under TRIA. For example, the Colonial Pipeline attack in May 2021, which caused gasoline shortages in the southeast United States, could have had much larger effects that affected other sectors if it had lasted longer. Any ripple effect in other sectors felt by the Colonial Pipeline attack would have been difficult to attribute to the specific Colonial Pipeline attack.

The Committee's letter to FIO (dated May 16, 2022) outlined issues related to TRIA:

- Cyberattacks do not respect geographic boundaries and can expand across many nations. As such, foreign events that cause damage to an organization within the United States such as 2017's NotPetya attack should be considered for inclusion under TRIA. Currently, the program may lead to many scenarios where a cyberattack outside the United States would lead to substantial damage and losses within the United States. In general, providing coverage under TRIA for damage inside the United States from a foreign event would be best considered as a type of loss that was envisioned to fall under the umbrella of coverages under TRIA. The Committee believes that such foreign events would meet the intent of covered damage under TRIA and as such should be covered. A clear example of how an attack with specific targets in one country can quickly become a global catastrophe is the 2017 NotPetya attack.

- Attribution surrounding cyberattacks is difficult to determine, pointing to a key topic in analyzing the interaction between TRIA and cyber insurance—a requirement is to understand which terrorist group caused the cyberattack. Given the nature of cyberattacks, often the exact source, timing, and motivation are not clear, at least for some period of time. Additionally, an attack on a particular target may, perhaps not purposefully, spread the damage to others. Again, the NotPetya attack is an example.

  Specific guidance on which types of attacks are considered terrorism, and the relevance of the involvement of foreign governments in determining whether an act is considered terrorism or "war," would provide needed clarity. It would be valuable to examine various scenarios and consider which types of events would be covered under TRIA and which would not. TRIA includes several requirements to trigger the payout of federal funds. One of these is a public finding by the secretary of the Treasury that an event was caused by nongovernmental terrorists. The difficulty of identifying the origin of a cyberattack, the likely ambiguity about the status of the attackers, and the length of time that it may take to get a public declaration about the identity of the attackers all suggest that there will be a great deal of uncertainty about the application of TRIA in the event of a major cyberattack. Consequently, the Committee believes that a different standard for certifying cyberattacks should be considered—one that does not require the identification of the attackers.

- Coverages included within TRIA are property and casualty insurance as defined under Part 50 subpart A[2] as noted below. These definitions are also reiterated in the June 2021 proposed definitional changes to TRIA.[3]

  (1) Means commercial lines within only the following lines of insurance from the NAIC's Exhibit of Premiums and Losses (commonly known as Statutory Page 14): Line 1—Fire; Line 2.1—Allied Lines; Line 5.1—Commercial Multiple Peril (non-liability portion); Line 5.2—Commercial Multiple Peril (liability portion); Line 8—Ocean Marine; Line 9—Inland Marine; Line 16—Workers' Compensation; Line 17—Other Liability; Line 18—Products Liability; Line 22—Aircraft (all perils); and Line 27—Boiler and Machinery; a stand-alone cyber liability policy falling within Line 17—Other Liability, is property and casualty insurance, so long as it is not otherwise identified for state reporting purposes as a policy that is not property and casualty insurance, such as professional liability insurance.

  (NAIC = National Association of Insurance Commissioners)

  It is important to note that professional liability insurance is still explicitly excluded from coverage under TRIA. Given that organizations may protect themselves from cyber

[2] https://www.ecfr.gov/current/title-31/subtitle-A/part-50/subpart-A/section-50.4
[3] https://www.federalregister.gov/documents/2021/06/09/2021-12014/terrorism-risk-insurance-program-updated-regulations-in-light-of-the-terrorism-risk-insurance#citation-14-p30538

incidents by utilizing terms and endorsements within professional liability insurance policy forms, this is a potential area of exploration regarding the modification of the lines of insurance covered within TRIA, especially as it relates to cyber-related losses.

U.S. Cyber Insurance Market

On the whole, the cyber insurance market is relatively young. Per the NAIC's 2021 Cyber Supplement, the total U.S. direct written premium for year end 2021 was $6.5 billion for all insurers. Excluding the $1.7 billion written by foreign surplus lines carriers, the domestic market accounts for $4.8 billion of premium. By comparison, the U.S. domestic property and casualty insurance (P&C) market wrote nearly $800 billion of premium in 2021 for all lines of insurance combined. While cyber insurance is clearly a developing and growing line of business, it still represents a relatively small portion (0.6%) of the domestic market for P&C coverages. However, the small size should not diminish the importance of the need for cyber insurance. The demand is likely to remain strong, and it is reasonable to expect ongoing outsized growth. This is due in large measure to the fact that the digital world and that cybercrime continue to expand and evolve. The combination of the two leads to strong demand growth for cyber coverage.

Due to the relatively small premium size of the cyber insurance market and the ever-changing nature of cybercrime, results for this nascent line have been volatile. The NAIC report shows that the average industry loss ratio for the last five years has ranged from 32% up to 66%. The highest loss ratio has occurred in each of the past two years (2020, 2021). This, related back to the evolution of cybercrime, has been caused by a greater incidence of ransomware attacks. The deterioration in loss experience in the most recent two years has been in spite of significant rate increases that occurred throughout 2021 and into 2022. Coverage terms have been tightened and insurers have demanded a more robust security posture due to the deterioration of loss results.

In light of the potential catastrophic exposure of the cyber line, it is important to understand the insurance industry's capacity. One common way to quantify this capacity is the industry surplus (capital base). Insurance premiums are estimated and set so as to fund the expected losses and expenses of the insurance risk transfer. This estimation is done at some point prior to when an insurance policy is issued and goes into effect. Surplus provides a buffer should those a priori estimates and resulting premiums prove to be insufficient in the near term. In short, surplus allows the industry to absorb unexpected losses, and it provides a level of safety to the customers relying on the insurance market. The U.S. P&C surplus for all domestic companies was just over $1 trillion at the end of 2021. This may not reflect additional surplus available from some reinsurers. Owing to a number of factors (natural disasters, inflation, increasing interest rates, stock market volatility, etc.), the total surplus has declined through midyear 2022. Insurers manage their risks and generally deploy their capital prudently. As such, not all capital could be earmarked for a single line of business. Further, individual insurers manage their aggregation of exposure to large loss events (such as hurricanes) to hopefully avoid large capital drawdowns. This aggregation management is accomplished through models that measure the exposure to large events and through the use of reinsurance.

Cyber Catastrophes

Unlike natural catastrophe risk, cyber risk comes with a rapidly changing landscape where bad actors seek to identify high-value and/or opportunistic targets and also change the type of attack and malware. Additionally, the same cyber events can be used globally almost simultaneously.

To mitigate risk, insurers and reinsurers look to diversify their portfolios. It should be noted that traditionally insurance companies might enter swaps with other carriers to diversity sector exposure and/or geographic exposure, believing if one sector or geography has a problem, it's likely another will not sustain a loss. However, the same cyberattack can be deployed on a large financial institution based in Florida with hurricane exposure as in California against a bakery with earthquake exposure as long as these firms share a common internet infrastructure or use the same software.

A distinguishing feature of cyber risk is that cyber catastrophes are typically manmade. An active adversary and motivational aspects of cyberattacks affect which entities are targeted. While people can be evacuated from the expected path of a hurricane to reduce the risk of harm, an active cyber adversary can adapt new tactics to cause damage that are not anticipated. Cyber catastrophic losses are also not isolated in confronting further risks. An earthquake in California may hardly influence expectations for the landfall of a hurricane in Florida, but a major cyberattack may expose new vulnerabilities, leading to further attacks. To quantify cyber accumulation risk, a simple and very conservative approach is to aggregate full insurance policy limits for the entire insurance portfolio. Beyond this, there are two main approaches to model accumulation: deterministic and probabilistic. To consider the impact and probable cost of a catastrophic cyber incident, it is important to consider the impact of recent experience.

NotPetya was the most expensive cyberattack ever. NotPetya caused over $10 billion in damages due to lost business, repairs, and other operational disruptions. The June 27, 2017, NotPetya cyberattack has been attributed to Russia's military intelligence deployed as part of the Ukrainian conflict. Russian hackers attacked the updater process of Ukrainian accounting software, MEDoc, and delivered NotPetya to MEDoc customers. The malware was built for speed as it spread across systems exploiting a single unprotected machine to then infect machines across a network and rapidly spread around the world.

In the spring of 2017, Russian military hackers were able to create a hidden back door into computers around the world that had MEDoc installed. When NotPetya was released, it spread automatically, rapidly, and indiscriminately. NotPetya irreversibly encrypted computers' boot records. No key existed to repair the computers. Multinational companies including Maersk, Merck, TNT Express, Saint-Gobain, Mondelez, and Reckitt Benckiser were victims of the attack. Approximate costs[4] of the damage for these companies (as of August 2018) were:

- Merck $870,000,000
- TNT Express (FedEx's European subsidiary) $400,000,000
- Saint-Gobain $384,000,000

[4] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

- Maersk $300,000,000
- Mondelez $188,000,000
- Reckitt Benckiser $129,000,000

These amounts do not include impacts that are harder to measure such as Maersk's disruption to the global supply chain, the inability of Merck to manufacture some medications, or any reputational damage.

Merck sued its insurers (Merck & Co. Inc. vs. Ace American Insurance Co. et al., N.J. Super. Ct., No. L-002682-18, summary judgment 1/13/22) for $1.4 billion after denial of coverage for the impact of NotPetya to their computer systems. The denial was due to the act of war exclusion, but the New Jersey Superior Court ruled against the exclusion. The reasoning was that the war exclusion is meant to apply to armed conflict and Merck was not informed that the cyberattacks would not be covered.[5]

A lawsuit was filed by Mondelez in October 2018 for $100 million against its insurer, Zurich. The insurance policy involved was not a cyber insurance policy, but rather a property insurance policy. Mondelez noted that the policy covered "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of machine code or instruction." Zurich relied on the war exclusion for denial of the claim. The claim was for the permanent damage to 1,700 servers, 24,000 laptops, unfulfilled orders, and other disruptions. The litigation was recently settled in a private agreement between the two parties.[6]

The Colonial Pipeline ransomware attack in May 2021 is the largest known cyberattack against the U.S. critical infrastructure. The initial access and data theft took place on May 6. Ransomware attack began the next day. President Biden declared an emergency on May 12.

The hack infected some of the Colonial Pipeline systems and shut down its operations for several days. The shutdown affected consumers and businesses on the East Coast. The pipeline supplies almost half of the fuel for the East Coast; systems that actually move oil were not directly compromised during the attack. DarkSide, believed to be operating out of Eastern Europe or Russia with no confirmed link to a nation-state, is thought to have been behind the attack. DarkSide mainly provides its services to other bad actors, allowing others to use its service against victims.

The attackers stole 100 gigabytes of data within a two-hour window. Following the data theft, the attackers infected the Colonial Pipeline IT network with ransomware that affected many

[5] https://news.bloomberglaw.com/privacy-and-data-security/mercks-1-4-billion-insurance-win-splits-cyber-from-act-of-war

[6] https://www.csoonline.com/article/3678970/mondelez-and-zurich-s-notpetya-cyber-attack-insurance-settlement-leaves-behind-no-legal-precedent.html

computer systems, including billing and accounting. The pipeline was shut down to prevent the ransomware from spreading.

The impact of the attack was significant, causing fuel shortages for many airlines with disruption at airports. Panic-buying and long lines at gas stations impacted many states, and gas prices spiked.

The attackers asked for approximately $4.4 million in bitcoin. The company paid the ransom, not being sure about the extent of penetration and the timeline to restore impacted systems. The Department of Justice recovered approximately $2.3 million from the attackers.

While the total cost of the damage just to Colonial is not clear, the company sued its insurer and stated "that it suffered more than $25 million in covered losses, and it paid the Alabama Department of Environmental Management $3.3 million for the release of petroleum product."[7]

Cyber Risk Models

Like catastrophe modeling for hurricanes, the cyber insurance market has undertaken to develop cyber models to measure aggregated losses and manage the exposure to large events. However, these latter models are far less mature in their development that other insurance risk models which are based on much longer experience and data.

Cyber risk models help the insurance industry attempt to quantify risk due to various types of cyber events. Cyber risk and cyber insurance are very new, as such modelling firms are rapidly modifying their models to blend industry expert opinion as well as (limited) historical experience. It should be noted that financial projections from the various insurers can be substantially different due to the rapidly evolving cyber landscape and the unique challenges for the insurance industry that cyber presents. The financial projections from a single firm can also vary significantly from one model iteration to the next as new information becomes available, views of the risk shift and also some coverages are changed.

At the March 2019 CAT Risk Management and Modelling Conference held in London, the first public cyber model comparison exercise was completed. Cyber model vendors were each provided with a common portfolio of 46 U.S. companies and a standard cyber insurance policy to model. The results of the models showed significant variation, indicating that the industry has not yet reached a consensus on accumulation modeling assumptions or its approach. As the industry matures, similar comparisons will likely continue to be performed for different cyber accumulation models. Additionally, given data challenges and the ongoing evolution of the nature of cyber risk, a vendor's model output may vary significantly from one version of its model to the next.

Vendors providing cyber accumulation modeling services can be broadly grouped into two camps: traditional catastrophe insurance modelers expanding into cyber risks, and the typically

[7] https://news.bloomberglaw.com/environment-and-energy/colonial-pipeline-insurer-aig-settle-suit-over-explosion-costs

newer cyber risk service providers moving into insurance. Generally speaking, the natural strengths and weaknesses of each type of vendor have become less pronounced as they are quickly learning from each other and the cyber market matures.

Many cyber accumulation model vendors were originally IT service providers, and they tend to have more in-house cyber expertise. Where data is sparse, expert judgment becomes increasingly important for assessing the next big emerging risk in the cyber domain, as well as staying on top of the dynamic landscape. Different models provide different degrees and types of flexibility in customizing parameters to reflect different views on cyber risk.

Due to data reporting requirements and data collection methods, data may have a bias toward newsworthy, data breach events. Many cyber model vendors partner with others and incorporate multiple other data sources including outside-in scans (gathered from the public space), inside-out scans (gathered from an organization's internal network), threat monitoring (vulnerabilities on the surface, deep and dark webs) and firmographic data (company characteristics such as revenue and employee count).

Many vendors have built their databases though internal efforts and in partnership with others. Some vendors hire teams of "white hat" hackers to map out company networks and direct the types of data captured. Other creative methods include scraping online IT job ad requirements to make inferences about a particular organization's software and systems. The fact remains, however, that many small companies are still not included in these databases, and one may need to adopt a deterministic market share approach as a result. However, the small company databases are growing quickly as more vendors target small businesses in their initiatives.

Accumulation modeling, and cyber risk modeling in general, are very active fields of endeavor and consequently subject to continual redevelopment and improvement. This means that the relative strengths and weaknesses of each vendor's products can be expected to shift and change over time. From an insurance writer's perspective, it may well be the case that no single vendor is able to completely capture cyber accumulation risk with a high degree of comfort. Inevitably, the cost to build and maintain models is a major factor to consider. Because of the difficulties that underlie accumulation risk modeling, managing the exposure may be as important as trying to accurately measure the risk.

Other Considerations

As FIO weighs considerations around a potential federal insurance response, we call to your attention the following:

- The current maturity level of the cyber insurance market should be factored in. While the market will undoubtedly continue to evolve, the current cyber insurance market will be subject to prudent risk and capacity management by insurers participating in the market.
- Consideration should be given to the potential and likely size of significant cyberattacks and clarifying the TRIA mechanism to address such an event.
- Further investment by the public sector and private entities in cyber security and risk mitigation should be encouraged.

The American Academy of Actuaries Committee on Cyber Risk appreciates that the Department of the Treasury is further considering concerns on cyber risk. We look forward to working with you and the Treasury staff to explore this topic.

If you have any questions about this letter or seek additional information from the Academy, contact Rob Fischer, casualty policy analyst, at fischer@actuary.org.

Sincerely,

Norman Niami, MAAA, FCAS, Affiliate IFoA
Chairperson
Committee on Cyber Risk