The University at Albany community has made this article openly available. Please share how this access benefits you.

Follow this and additional works at: https://scholarsarchive.library.albany.edu/honorscollege_pos

Part of the Political Science Commons

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License Rights Statement
The Insurer of Last Resort: Investigating a Federal Insurance Backstop for Catastrophic Cyber Incidents

An honors thesis presented to the Department of Political Science, University at Albany, State University of New York in partial fulfillment of the requirements for graduation with Honors in Political Science and graduation from The Honors College

Brianna L. Bace
Research Mentor: Unal Tatar, Ph.D.
Research Advisor: Zsofia Barta, Ph.D.

May 2023
Abstract

The demand for cyber insurance has accelerated in recent years due to the increased frequency and severity of cyber-attacks. The NotPeyta cyberattack, which spread to countries and systems across the globe and is estimated to have caused over $10 billion in damages, is one example. These kinds of catastrophic cyber incidents are causing insurers to raise premiums and tighten their policies, creating a significant gap in protection in the market. In response to this problem, the United States Treasury Department issued a Request for Comment regarding the potential for a federal insurance response to catastrophic cyber incidents.

The aim of this thesis is to investigate what a federal backstop for cyber insurance could look like and how different groups feel about its potential creation. I analyze the submitted comments and additional open-source information to assess the opinions that the U.S. government and the cybersecurity and insurance industries each have towards a federal backstop. Looking specifically at opinions on the scope of coverage, catastrophe threshold, and policyholder requirements, I determine that while all three groups support its creation, there is significant variation in how each group pictures a federal backstop.

Keywords: cyber insurance market, catastrophic cyber incidents, federal backstop, cyber risk, Terrorism Risk Insurance Program (TRIP)
Acknowledgement

The completion of this thesis would not have been possible without the exceptional support of many wonderful individuals. I would like to express my deepest appreciation and thanks to my research mentor Dr. Tatar for his support and encouragement not only during this project, but over the course of my undergraduate education. Dr. Tatar has provided me with numerous opportunities that have helped me to grow as a person and as a cybersecurity professional.

I would like to extend my thanks to Dr. Barta. Her insight and feedback over this past year has made me a better writer and researcher. I am also extremely grateful to Professor Turetsky for his professional guidance and support.

Most of all, I would like to thank my mom and my brother, whose love and guidance is with me in everything I pursue. Thank you for your endless encouragement.
# Table of Contents

Abstract ............................................................................................................................... ii  
Acknowledgement ................................................................................................................ iii  

Introduction ......................................................................................................................... 1  

Cyber Insurance .................................................................................................................. 3  

Methodology ....................................................................................................................... 6  
   A. Data .............................................................................................................................. 6  
   B. Analysis Approach ...................................................................................................... 6  

Picturing a Federal Backstop ............................................................................................... 6  
   A. Scope ........................................................................................................................... 8  
   B. Catastrophe Threshold .............................................................................................. 9  
   C. Requirements ............................................................................................................. 10  

Opinions on a Federal Backstop ......................................................................................... 11  
   A. Government ............................................................................................................... 12  
   B. Cybersecurity Industry ............................................................................................. 14  
   C. Insurance Industry ................................................................................................... 15  
   D. Who’s Paying ............................................................................................................ 18  

Conclusion .......................................................................................................................... 20  

References .......................................................................................................................... 21  

Introduction

Cyberattacks have the capacity to cause significant damage across industries, sectors, and societies. Systemic cyber incidents\(^1\) or attacks that spill over from their initial target into other firms, especially those that are economically linked, pose a serious cyber risk. The 2017 NotPeyta malware attack was a systemic cyber incident, as the data-destroying malware deployed by Russia against Ukraine spread outside of Ukraine to other companies and systems across the globe. It is estimated that this attack led to $10 billion in damages (Greenberg, 2018), making it the closest example of a catastrophic cyber incident\(^2\) to date.

The demand for cyber insurance\(^3\) has accelerated as the frequency and severity of cyberattacks have increased. Due to the high expense that cyberattacks carry, cyber insurance is an important component in the resiliency of a company post-attack. The losses that catastrophic cyber incidents can incur are even more significant, reaching billions of dollars. Now, as the plausibility of catastrophic cyber incidents grows, the existence of the cyber insurance market is being threatened. A growing number of insurers feel these incidents are “beyond the risk appetite and capacity of the private cyber insurance market” (Institute of International Finance, 2022, p.2). The threat of catastrophic cyber incidents can cause the demand for cyber risk limits to exceed the capacity of the cyber insurance market.

---

\(^1\) The Department of Homeland Security defines cyber incidents as “incident occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon,” (DHS, 2017, pp.140-141).

\(^2\) Though a final definition has yet to be established for a catastrophic cyber incident, one expert panel made up of panelists representing actuarial sciences, the insurance industry, the risk management domain, the cybersecurity domain, and academia believed that economic impact, network effect, and severity are three distinct measures that makes a catastrophic cyber risk. Physical manifestation, irreversibility, and systemic nature were additional dimensions (Tatar et al., 2023a).

\(^3\) Cyber insurance is a risk-transfer mechanism used to provide coverage for losses, damages, and costs incurred due to cyber incidents.
In response to this issue, the Government Accountability Office (GAO) published a report in June 2022 recommending the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Insurance Office (FIO) “to jointly assess the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response,” (GAO, 2022, para. 12). In response to the GAO’s recommendation, the FIO in the Treasury Department issued a Request for Comment\(^4\) regarding the potential creation of a federal insurance response to catastrophic cyber incidents. The U.S. government has a long history of creating federal insurance programs, such as the terrorism risk insurance program (TRIP), the National Flood Insurance Program (NFIP), and the Federal Crop Insurance Program (FCIP). These programs are mechanisms for the FIO to provide federal assistance for coverage of catastrophic incidents caused by natural disasters or acts of terrorism. Essentially, the U.S. government becomes an insurer of last resort, taking on the risk that the private insurance market cannot handle through the creation of a backstop.

The aim of this thesis is to investigate what a federal backstop for cyber insurance could look like and how different groups (e.g. the U.S. government, the cybersecurity industry, and the insurance industry) think about its potential creation. In this paper, I perform a desk review on the topic of cyber insurance and a potential federal insurance response to catastrophic cyber incidents. I also perform a document analysis on the comments submitted to the FIO following their Request for Comment in order to assess the attitudes that different industries and sectors have towards a potential backstop for cyber insurance. I begin this paper with further analysis of the problem impacting the cyber insurance market, namely its hardening in recent years.

\(^4\) (U.S. Treasury Department, 2022)
Cyber Insurance

The cyber insurance market has been around for about 20 years and is constantly evolving. As of 2020, approximately $4 billion in direct premiums have been written by the cyber insurance market (FIO, 2022). Today, the U.S. has the largest market for cyber insurance in the world. Cyber insurance is one part of the larger property and casualty (P&C) insurance market, with policies coming in three main forms: third-party written coverage, first-party written coverage\(^5\), and implicit silent cyber coverage\(^6\). In the early years of the cyber insurance industry, cyber insurance was traditionally packaged into commercial P&C policies. Today, it is also common to see cyber insurance offered as a separate policy, especially in certain sectors. Standalone insurance policies are more likely to be adopted by the education (66%), healthcare (62%), and technology and communications (51%) sectors, then by the finance (27%), manufacturing (30%), and retail (39%) sectors (Granato & Polacek, 2019, para.8). About 58% of large businesses have a standalone cyber insurance policy, compared with just 21% of small businesses (Granato & Polacek, 2019, para.8).

Cyber incidents are not just an issue for underwriters of cyber insurance policies; they are a significant problem for underwriters of non-cyber policies as well due to “non-affirmative” or “silent” risk. Silent risk can reside in many different types of policies, even policies written by insurers that write little or no cyber insurance policies. According to a 2020 global survey, 65% of underwriters were concerned about silent cyber coverage exposure in P&C policies (Department of Financial Services, 2021). This is a valid concern as $2.7 billion of the $3 billion

\(^5\) Third-party coverage policies include coverage for privacy liability, network security liability, and privacy regulatory defense costs, while first-party liability can include extortion, ransomware, and business interruption coverage.

\(^6\) Silent cyber coverage is not actually a cyber insurance policy. It a term that refers to potential cyber-related losses stemming from traditional property and casualty policies that neither explicitly include nor exclude cyber coverage or coverage of cybersecurity events (Tatar et al., 2021).
insurance claims that came from the 2017 NotPeyta attack were made under P&C policies that did not explicitly cover cyber risks (Department of Financial Services, 2021).

Cyberattacks like NotPetya and WannaCry⁷ have contributed to the significant hardening of the cyber insurance market. In the insurance business, it is better to have a soft market than a hard one, as hardening can cause changes to prices, terms, and conditions, as well as the availability of coverage and capacity (Kresse, 2021). Specifically for the cyber insurance market, the price of premiums, deductibles, and retentions has increased, while policy coverage in areas of extortion and exclusions for nation-state attacks has tightened. We saw this in the months following the 2017 NotPeyta attack. Mondelez International, a multinational food company based in Chicago, was a victim of the NotPeyta attack, with losses totaling more than $180 million for the company (Mondelez v. Zurich, 2018). After the attack, Mondelez, who has an all-risk property insurance policy with Zurich American Insurance, filed an insurance claim seeking compensation for their NotPeyta losses. Zurich denied the claim and refused to provide coverage for damages by invoking the “hostile or warlike action” exclusion (Mondelez v. Zurich, 2018). After a four-year legal battle, both parties came to a settlement at the end of 2022, before a judge could make a definitive ruling on the issue of war exclusions.

Most cyber insurance policies, like the one Mondelez had with Zurich, contain a war exclusion to protect against catastrophic losses. The issue is that war exclusion language is currently being updated by many insurers in a way in which losses from widespread/systemic incidents caused by zero-day vulnerabilities, cloud outages, self-propagating malware, etc., would also not be covered by the insurer (CyberAcuView, 2022b). For example, starting this

⁷ WannaCry was a ransomware attack that spread to more than 200,000 computers in over 150 countries in May 2017. One notable victim was the United Kingdom’s National Health Service (NHS), where “thousands of appointments and operations were cancelled and in five areas patients had to travel further to accident and emergency departments” (National Audit Office, 2017, para.5) due to the attack.
year, Lloyd’s of London, one of the world’s leading insurance and reinsurance marketplace, made a move to require its insurance groups to “exclude” nation-state cyber-attacks from their cyber insurance policies (Rundle, 2022). As new exclusions are created, and old exclusions are expanded, protection gaps will be an increasing issue for the cyber insurance market.

The NotPeyta attack is just one reason we have seen a hardening in the cyber insurance market. Other reasons include “the evolving threat landscape of ransomware activity, the changing legal and regulatory issues generally related to wrongful collection and widespread IT supply chain attacks” (Sylvester, n.d., para.2). The scalability of cyberattacks is another contributing factor, as one attack could affect thousands of firms simultaneously, causing significant interrelated losses for insurers (Granato & Polacek, 2019). For example, Lloyd’s of London released a report in which they estimated that a cyberattack on the U.S. East Coast power grid could result in $243 billion to $1 trillion in economic losses and $21.4 to $71 billion in insurance industry losses, primarily from business interruption and property damage (Lloyd’s, 2015). The lack of actuarial data is yet another persistent problem for insurers, as it has kept them from accurately pricing risk (Knake, 2016). Without this data, insurers will continue to avoid risk by limiting their policies.

With estimates for the industry’s global cyber risk exposure already in the region of $150 billion (PWC, 2015), there is no better time to discuss the potential need for a federal backstop for catastrophic cyber incidents. A federal backstop could combat limitations under current insurance coverage policies and help reduce the uncertainty in the market that is causing insurers to tighten policies.
Methodology

Data

The Treasury Department’s Request for Comment regarding a potential federal insurance response to catastrophic cyber incidents was filed on September 28, 2022, with submissions open until December 14, 2022. The public had just under three months to submit their comments to answer the FIO’s questions on this issue and provide additional information relating to cyber insurance and catastrophic cyber incidents. A total of 59 comments were submitted from private citizens and firms from several different industries, including but not limited to cybersecurity and insurance. Several of the comments are referenced throughout this thesis.

Analysis Approach

In this thesis, I perform a document analysis of the comments submitted in response to the FIO’s Request for Comment. Specifically, I look at the responses from companies and other firms within the cybersecurity or insurance industries. I also perform a desk review on the topics of cyber insurance and catastrophic cyber incidents, which includes a review of the U.S. government’s stance on a potential federal insurance response to catastrophic cyber incidents in the form of a backstop.

Picturing a Federal Backstop

One reason why supporters of a cyber insurance federal backstop believe in its success is due to the federal government’s history of stepping in and providing federal assistance for coverage of catastrophic incidents via federal insurance programs. The Terrorism Risk Insurance Program (TRIP) was established by the Terrorism Risk Insurance Act (TRIA) of 2002 following the 9/11 terrorist attacks when coverage for acts of terrorism became impossible to obtain.
TRIP/TRIA is especially important when discussing catastrophic cyber incident coverage as the Treasury Department has a “longstanding interest in terrorism risk insurance for cyber losses and its implications for the administration of TRIP” (FIO, 2022, p.58). The Treasury has confirmed that requirements found in TRIA apply to any policy covering cyber risk written in a line of insurance subject to TRIP. This means that TRIP can be triggered if a policy does not specifically exclude losses arising from a cyber event. To maintain this possibility, some insurers have worked to create carveouts in their policies for cyber incidents certified by the Treasury as acts of terrorism, as many war exclusions already extend beyond war to “encompass a range of hostile activity that could include crime, political unrest, and terrorism” (FIO, 2022, p.61) Some believe that TRIP/TRIA is the solution to the catastrophic cyber risk problem, and that with the addition of cyber definitions to the TRIA, there is no need for a separate cyber risk federal backstop. Unfortunately, there are several issues with this plan.

For TRIP to be triggered, the incident must be a “certified act of terrorism.” Achieving this certification would be extremely difficult for a cyber incident as TRIA requires that the incident be violent or dangerous to human life, property, or infrastructure. While it is certainly true that cyberattacks can be violent or dangerous, especially if the attack takes place against critical infrastructure, not all cyber-attacks have these types of impacts. Instead, cyber-attacks cause significant business impacts and monetary losses due to exfiltrated data or disruptions to command-and-control systems. These types of behaviors are serious but not necessarily violent.

Another impediment to triggering TRIP is that a significant amount of cyber coverage is included in non-stand-alone insurance policies, which are specifically excluded from TRIA. Further, experts believe that it would be “legislatively awkward” (Cunningham & Talesh, 2021,

---

8 TRIP-Eligible lines of insurance includes commercial P&C insurance that is subject to TRIP pursuant to 31 C.F.R. § 50.4(w) (FIO, 2022).
p.50) to add cyber provisions into TRIA that only apply to catastrophic cyber incidents. To clear up significant legal uncertainty and challenges, a federal backstop built specifically for cyber risk is needed. This will require determining the scope of coverage, setting a catastrophe threshold, and creating the requirements for coverage.

**Scope**

A successful federal backstop created for cyber could cover more than the standalone cyber risk policies that TRIA would. Researchers Cunningham & Talesh (2021) believe that a federal backstop for cyber should apply to any policy which explicitly includes cyber risk coverage. A backstop for cyber insurance could also feature agreed-upon definitions for terminology that currently causes significant uncertainty in the market. Just defining catastrophic cyber risk is a challenge as insurers and insureds look at it in different ways. For example, insureds or those covered by an insurance policy may define catastrophic cyber risk as “one that has an economic impact, network effect, and damages to their business mission, individuals, or financial outlooks,” (Tatar et al., 2023a, p.12). This is different than insurers, who may define it more so as a systemic vulnerability that leads to widespread incidents and claims. Even in different departments of government, “catastrophic” means different things. If a catastrophic cyber incident happened today, it would be unclear who in government would be responding as one department’s catastrophic may not be another department’s catastrophic (Tatar et al., 2023b). Providing definitions would greatly decrease uncertainty by helping insurers to make informed choices about their levels of coverage, insureds to be certain of their insurance coverage (Carter & Enoizi, 2020) and government to know how exactly to respond. Furthermore, a backstop could be used to clear up the legal and contractual uncertainty that surrounds attribution and coverage exclusions for catastrophic cyber incidents. If the government clearly articulated which types of
cyber incidents were and were not covered, then future insurers and insureds would not have to engage in legal battles like the one we saw happen between Mondelez International and Zurich⁹. While insurers should also work to clearly differentiate various cyber risks and respond accordingly to the changing cyber threat landscape (Tatar et al., 2021), a backstop could also aid in this process.

**Catastrophe Threshold**

Another important component of a federal backstop is its catastrophe threshold or the number that losses must reach to trigger a payout. Thresholds that currently exist in cyber policies and in TRIA are insufficient for catastrophic cyber incidents. Existing cybersecurity policies typically cover between $10 million to $500 million, depending on the product and provider (Eling & Schnell, 2016). TRIA’s threshold is considered a very high threshold at $200 million. But even after its $40 million increase between 2018 and 2020, TRIA’s threshold is still an inappropriate threshold for catastrophic cyber incidents that are predicted to reach billions of dollars.

Though there is a lack of sufficient data, previous systemic cyber incidents provide us with a rough estimate of what the threshold should look like. Though the NotPeyta attack impacted more than just the United States, it demonstrated the potential monetary impact of a cyberattack that spreads across industries and infrastructure. For that reason, a catastrophe threshold of $10 billion would make sense as this is the estimated total losses incurred by NotPeyta (Greenberg, 2018). Researchers Cunningham & Talesh (2021), who created a proposal for a federal government financial backstop for cyber called the “Catastrophic Cyberattack

⁹ (Mondelez v. Zurich, 2018).
Resilience Act (CCRA),” believe an initial allotment of $10 billion is fair, with additional appropriations capping out at $50 billion. A threshold of this magnitude can provide “much-needed confidence in the long-term cyber insurance market,” (p.41). Determining an appropriate threshold will require significant consideration and further data collection.

Requirements

All federal backstops have requirements that must be met for the payout to occur. In TRIA, one type of requirement is the general disclosure requirement on insurers. An insurer must disclose to the policyholder the premium charged for insured losses covered by TRIP and the Federal share of compensation for insured losses under the Program (U.S. Treasury Department, 2002). As for a federal backstop for cyber, the government appears to be exploring adding cybersecurity measures into a backstop. If added, the policyholder would need to prove that it has met certain cybersecurity standards to be covered. This type of requirement would directly combat the moral hazard problem, or the phenomenon in which those who are insured take advantage of the fact that they have insurance and engage in dangerous or risky behavior that they otherwise would not. The inclusion of mandatory cyber hygiene measures would combat this problem by ensuring no company is taking unnecessary risks by operating without at least a basic level of security. By incentivizing greater cyber resiliency, firms will become more resilient to cyberattacks, and so the likelihood of a catastrophic cyber incident decreases. For example, The Cyberspace Solarium Commission recommended incentivizing timely patch implementation\(^\text{10}\) by placing a cap on insurance payouts for incidents that involved unpatched systems.

\(^\text{10}\) This is recommendation 4.2.1 of the Cyberspace Solarium Commission report.
If a federal backstop was to be created and cyber hygiene measures were to be a main requirement of coverage, there would have to be a consensus on what these measures would be. What does a basic level of security look like? For Marsh, an insurance company operating in 130 countries, its underwriters use a list of twelve cybersecurity controls\(^\text{11}\) to assess an applicant’s cyber operating environment. But for another insurer, these controls could be different. A key part of creating a federal backstop will be finding consensus regarding cyber hygiene measures and any other requirements that the government may look to add.

**Opinions on a Federal Backstop**

In the United States, the potential for a federal backstop for cyber insurance is a major public policy issue as several of the leading global cyber insurance providers operate out of the U.S. Just ten firms\(^\text{12}\) wrote almost 68% the cyber insurance market in 2020, with premiums totaling approximately $1.86 billion (NAIC, 2021). Like with any public policy issue, firms in different industries or sectors have their own opinions and reservations regarding potential legislation that Congress may attempt to pass. The comments posted in response to the FIO’s Request for Comment give us insight into some of the opinions and reservations held about a federal backstop for cyber.

Generally, the comments submitted conveyed thanks to the FIO for recognizing the ongoing issues in the cyber insurance market. Many of the comments refrained from making definitive judgments on a federal backstop, stating that further comprehensive study should be

---

\(^{11}\) These controls include multifactor authentication; email filtering and web security; secured, tested, and encrypted backups, privileged access management (PAM); endpoint detection and response (EDR); patch and vulnerability management; incident response plans; cybersecurity awareness training and phishing testing; remote desktop protocol (RDP) mitigation and other hardening techniques; logging and monitoring, replacement or protection of end-of-life (EOL) systems; and digital supply chain cyber risk management (Marsh, 2022).

\(^{12}\) From smallest to largest market share, these firms include BCS, Hartford Fire & Cas, Fairfax Financial, CNA, AXIS, Beazley, Travelers, AIG, AXA XL, and Chubb (NAIC, 2021).
completed first. Nonetheless, a document review of the comments reveals that both the cybersecurity and the insurance industry have strong opinions regarding a federal backstop. These two industries, in addition to the views of the U.S. government, give us three distinct groups of opinions regarding a potential federal backstop for cyber insurance. Furthermore, due to the different motivations of these groups, each views a potential backstop in a slightly different way.

**Government**

For the government, a federal backstop for catastrophic cyber incidents would be a mechanism to provide stability to the private insurance market. Two different branches of government seem to not only recognize the importance of cyber insurance but agree that there is a need for a federal insurance response. The National Cybersecurity Strategy, which was released on March 2, 2023, signaled that the executive branch, including the White House, and several executive departments like the Department of Homeland Security and the Department of Commerce, all feel that a federal backstop may be one way to achieve greater cyber resiliency and certainty to American markets.

Congress also has a history of discussing cyber insurance. In February 2023, the Senate introduced a bill called the Insure Cybersecurity Act. If passed, the bill would direct the Assistant Secretary of Commerce for Communications and Information to establish a working group on cyber insurance (S.513, 2023). In 2016, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing on the potential role of the cyber insurance market in promoting better risk management. In this hearing, Chairman John Ratcliffe stated that he believed cyber insurance to be a market-driven method of advancing the
security of the nation (The Role of Cyber Insurance Risk Management, 2016). This hearing was evidence that policymakers and industry representatives have long felt that cyber insurance could motivate companies and other firms to assess their cyber practices and thus strengthen their cyber resiliency.

Unfortunately, while the cyber insurance market has grown significantly in recent years, we have yet to see cyber insurance achieve its potential to incentivize better cyber hygiene of the insured. Inadequate cybersecurity practices still exist throughout the United States. A 2021 U.S. Cybersecurity and Infrastructure Agency (CISA) report stated that victims, specifically those of cloud services attacks, were failing to employ basic cybersecurity protective techniques and train their employees against phishing attacks (CISA, 2021). The lack of improving cybersecurity likely indicates that the moral hazard problem could already be impacting the cyber insurance market. The National Flood Insurance Program (NFIP) is evidence that moral hazard can impact the success of a federal insurance response as the NFIP has unintentionally encouraged people to live in vulnerable flood-prone areas (Fox, 2023). The government will undoubtedly be concerned about repeating its mistakes in NFIP. Based on their history of creating cybersecurity frameworks and their recent commitment to implement “light-touch” cybersecurity regulations (Pattison-Gordon, 2023), it is highly likely that the government would include cybersecurity requirements for policyholders into a federal backstop. This way, the government can combat a moral hazard by rewarding good risk management behavior and refusing to insure companies with bad risk management behavior.

---

13 (NIST, 2018)
The responses by cybersecurity firms and groups analyzed in this thesis spoke positively of a potential federal backstop. Like the government, this industry sees a backstop as an opportunity to improve the cybersecurity of the nation through required cyber hygiene measures. Sentinel One, a cybersecurity company, named specific measures, such as multi-factor authentication, regular patching, back-ups, and cybersecurity training, as a few key cybersecurity defenses that the government can incentivize (SentinelOne, 2022). They also warned that creating a backstop without robust security standards and eligibility requirements could hinder the deployment of cybersecurity tools (SentinelOne, 2022). The Cybersecurity Coalition believes it is important that underwriting is not just market-driven but also driven by the policyholder’s due diligence (Cybersecurity Coalition, 2022). CyberCube recommends using the NIST Cybersecurity Framework and the Center for Internet Security’s Critical Security Controls to prove a policyholder’s due diligence and commitment to stronger risk management (Cybercube, 2022). CyberCube, a cyber risk analytics company, was also supportive of CyberAcuView’s endorsement of CISA’s Bad Practices List as a starting point for minimum cyber security best practices.

A few of the comments also spoke to a potential scope and threshold for the backstop. CyberCube believed that one way to define catastrophic incidents was through insurance-loss-driven metrics. This way, the government would not need to create definitions for attribution or infrastructure as would be required if catastrophic cyber incidents were defined based on the

14 The Cybersecurity Coalition is made up of nineteen companies including Broadcom, Cisco, Citrix, Cybastion, Cybereason, Gen, Google, Intel, Kroll Cyber Risk, Microsoft, Mozilla, Netscout, Palo Alto Networks, Rapid7, Red Hat, Resilience, Schneider Electric, Tenable, and Trellix (Cybersecurity Coalition, n.d.).
15 (CyberAcuView, 2022a)
involvement of nation-state actors or specific infrastructure. In their argument for defining a threshold, the company believes that a loss-ratio-based government backstop would be beneficial. In their example, a program that capped cyber insurance losses at either 265% of the premium in a market-wide loss event or 3% of industry limits could stabilize the market (CyberCube, 2022). Similar to CyberCube, Cowbell, a cyber insurance company, also supported a loss-ratio calculation. They proposed the idea of mimicking the economic trigger of TRIA in which the government covers 85% of losses above 20% of an individual insurer’s calendar year Earned Premium (Cowbell, 2022).

Both Cowbell and Good Harbor (a cybersecurity risk management company) emphasized in their comments that it would be more suitable for the federal government to take a public-private partnership approach than become the exclusive insurer or a competitor to the private market (Cowbell, 2022; Good Harbor & Cyber Re, 2022). Essentially, the program would have the government “sit on top of the primary markets and act temporarily as a reinsurer” (Cowbell, 2022, p.12) in the event of catastrophic cyber incidents. For Cowbell, the scope of a backstop would include the entire cyber market and its supply chain, while Good Harbor and Cyber Re specifically named high-severity systemic loss events and acts of cyber warfare as two areas where the private would need assistance absorbing losses (Good Harbor & Cyber Re, 2022). Even though, ideas for scope of coverage, catastrophe threshold, and policyholder requirements varied, the general attitude towards a backstop was hopeful as it would be a mechanism that provides stability to the market while improving cyber hygiene in companies at the same time.

**Insurance Industry**

Though there are aspects that the insurance industry generally supports, such as the addition of cyber hygiene measures for a potential backstop, the insurance industry seems to be a
bit more skeptical. The insurance industry is worried about potential strings attached. In public remarks made by one representative, there is opposition towards a backstop for fear that it would lead to too much regulation. For example, Jeremy Gittler, head of cyber and technology-Americas at AXA XL, stated that “we don’t want a situation where they’re [the federal government] saying … you can only deploy this much capacity, you have to get this much reinsurance…None of us want that” (Greenwald, 2023, para.3). In his statement, Gittler does go on to support the idea of a “true” federal backstop, one where the government only comes in and takes over after losses hit a specific number so that the insurance industry can survive. The insurance industry does not want a federal backstop to enable the federal government to step in and take over the market. Nor does the market want regulations put in place that could stifle innovation, impose costly burdens, and otherwise lessen the power they already have.

Due to their knowledge and expertise, there is also a recurring sentiment that the private insurance market is better and more capable of dealing with the exposure and risk than the government. Gittler also stated in his remarks that “we’re [insurance companies] the ones with the expertise, not those who work for the government” (Greenwald, 2023, para.2). Lloyd’s of London, an insurance market that currently writes 20% of global cyber insurance premiums, echoed this sentiment in their comment, stating that “Lloyd’s always believes private market solutions are preferable” (Lloyd’s, 2022,p.3). Lloyd’s eventually goes on to say that because the cyber insurance market has no appetite to cover catastrophic cyber risk, it makes sense to begin considering some type of federal response mechanism.

---

16 AXA XL is an insurance company that holds 12.8% of the US cyber insurance market (Littlejohns, 2019).
Though the insurance industry seems to share the opinion of the government and the cybersecurity industry that cyber hygiene requirements are important, there are still some differences. For example, Marsh McLennan stated that a defense-in-depth approach should be taken in all cases (Marsh McLennan, 2022). Yet, later in its comment, Marsh proposed that all policyholders be offered the buy-in for the backstop without required cyber hygiene measures, as the private market has already implemented a base level of cybersecurity requirements into their underwriting process (Marsh McLennan, 2022). The Reinsurance Association of America (RAA) said something similar in their comment. In answering how the federal government can incentivize policyholders to adopt cyber hygiene measures, the RAA stated that the federal government should not interfere with or otherwise mandate underwriting controls. Essentially, the RAA is against punishing policyholders for failing to meet minimum cybersecurity requirements (RAA, 2022). This is a different view to those in government and the cybersecurity industry who support the addition of cyber hygiene requirements in part because they would motivate companies to have a better cybersecurity posture out of fear of not qualifying for coverage.

In their comment, The National Association of Mutual Insurance Companies (NAMIC) supported efforts to accelerate multifactor authentication protections and recommended that the FIO work with CISA to identify “best practices to evaluate a potential insured’s cyber maturity during cyber underwriting and risk assessment processes,” (NAMIC, 2022, p.5). A few commenters, including Gallagher Re and Zurich, also emphasized the importance of making determinations of best practices and requirements an evolving process and not once and done implementation.
Gallagher Re also addressed the potential scope of coverage. Gallagher Re stated that a backstop should cover all U.S.-based and U.S.-owned overseas critical infrastructure assets, U.S. domiciled policyholders or global policyholders with U.S. subsidiaries, and incidents involving critical infrastructure and systemic war events (Gallagher Re, 2022). They did not recommend specific requirements around policyholders, such as size, as this would “exclude large portions of the economy from accessing a federal solution” (Gallagher Re, 2022, p.12). Marsh McLennan also commented on a scope of coverage, but in less detail, stating that a backstop should “extend beyond the current state insurance products” (Marsh McLennan 2022, p.16) and later adding that a backstop should include physical loss or damage, bodily injury, and financial loss.

When it came to proposing a threshold, very few firms in this group gave numerical estimates. Marsh McLennan was one firm that proposed a threshold for a backstop. They supported a floor of $100 billion to ensure public funds are only ever used in response to cyber incidents that pose “an existential threat to cyber insurance marketplace” (Marsh McLennan, 2022, p.7). Many of the comments did not specifically mention a threshold or merely stated that this was a difficult issue to quantify and further data would need to be collected. Overall, the comments from the insurance industry portrayed a general wariness towards government intervention in the form of a federal insurance response. Even though many firms saw the value in a backstop, there were still some aspects of their opinions, such as whether or not to make cyber hygiene requirements mandatory, differed from the opinions held by the government or the cybersecurity industry.

Who’s Paying?

If a federal cyber insurance program was created, someone would have to pay for it. This reality is an obvious point of contention in discussions of a federal backstop as it could be argued
that taxpayers would be on the hook for the negligence and bad cyber behavior of companies. Based on previous federal insurance responses, those footing the bill could be taxpayers or the industry, depending on the structure of the final backstop. For example, if TRIP was triggered, the losses paid by the Treasury Department would be recovered by a surcharge on nationwide property insurance premiums for urban, suburban, and rural properties (Woods, 2023). There is also precedent for backstops to be paid for by taxpayers, especially if it stabilizes a market used by the vast majority of citizens. Either option results in at least one unhappy group. Fortunately, some experts believe that if structured correctly, a backstop could help to prevent the likelihood of a payout. In their paper, Cunningham & Talesh (2021) suggest that if mandatory cyber hygiene measures were a part of the final backstop, then the vulnerability of covered companies would decrease, and so would the likelihood that they fall victim to a catastrophic cyber incident. This is similar to how measures put into place after 9/11 have prevented many terrorist attacks.

To date, TRIP/TRIA is considered a very successful policy in part because a payout has never been made.

Despite TRIA’s success, we have also seen failure in some federal insurance programs. The NFIP, for example, has led to a serious burden on taxpayers. The program owes the Treasury $23 billion and, in the view of the GAO, has no viable path to repay it based on premiums collected and projected payouts (Knake, 2016). There is some fear that “if developed incorrectly…[a cyber insurance backstop] could displace the private market and leave taxpayers to foot the bill” (Knake, 2016, para.9).

Marsh McLennan, Cowbell, and Gallagher Re made recommendations on how a federal backstop for cyber could be funded. Marsh recommended funding in advance through a percentage of premium, like TRIA, with no or a very limited opt-out provision (Marsh
McLennan, 2022). Cowbell also suggested pre-funding a backstop via a premium tax for the entire cyber industry. Gallagher Re felt that a potential backstop could be both pre and post pre- and post-funded with, in addition to other mechanisms, premiums on insureds and reinsureds so that they share the cost with the taxpayers (Gallagher Re, 2022).

Ultimately, it is too early to speak about how a backstop would be paid for – we can confidently say that adding requirements like mandatory cyber hygiene measures could reduce the likelihood of ever seeing a payout. As for those against an industry-wide levy, we can also confidently say that the cyber insurance market would be much better off paying a levy than dealing with a catastrophic cyber incident without a backstop.

**Conclusion**

As the frequency and severity of cyber-attacks increase and the potential for catastrophic cyber incidents rise, it is inevitable that the government is going to step in. Experts believe that it is better for the federal government to structure a response now than to wait until after a catastrophic incident has already occurred. Starting this process now will give the federal government time to work with state regulators and stakeholders in both the cybersecurity and insurance industries to produce a structure for a federal backstop that is beneficial to all parties. The submitted comments from firms in the cybersecurity and insurance industries show that there are places where the two industries both agree and disagree. Yet, broadly speaking, both groups support the creation of a federal backstop where the government takes on risk that the private market no longer wishes to over. While there is a fair deal of agreement across government and industry regarding the seriousness of a possible catastrophic cyber incident, the U.S. government should take advantage of this alignment and move ahead with becoming an insurer of last resort for the cyber insurance market.


The Role of Cyber Insurance in Risk Management, U.S. Subcommittee on Cybersecurity,

