

# Strategies and Solutions Against Catastrophic Cyber Incidents An Expert Panel Discussion

PART 4

JUNE | 2023





CASUALTY  
ACTUARIAL  
SOCIETY

# Strategies and Solutions Against Catastrophic Cyber Incidents

An Expert Panel Discussion

**AUTHORS** Unal Tatar, PhD  
Brian Nussbaum, PhD  
Omer F. Keskin, PhD  
Elisabeth Dubois, MBA, PMP  
Dominick Foti, MBA  
Brianna Bace  
Rian Davis

**SPONSOR** Catastrophe and Climate Strategic  
Research Program Steering Committee  
  
Casualty Actuarial Society



**Give us your feedback!**  
Take a short survey on this report.

[Click Here](#)



#### **Caveat and Disclaimer**

The opinions expressed and conclusions reached by the authors are their own and do not represent any official position or opinion of the Society of Actuaries Research Institute, the Society of Actuaries or its members. The Society of Actuaries Research Institute makes no representation or warranty to the accuracy of the information.

Copyright © 2023 by the Society of Actuaries Research Institute. All rights reserved.

# CONTENTS

- Executive Summary ..... 4**
- Section 1: Background, Objectives, and Method ..... 6**
- Section 2: Pre-Incident Challenges of Catastrophic Cyber Risks ..... 7**
- Section 3: Post-Incident Challenges of Catastrophic Cyber Risks..... 10**
- Section 4: The Role of Government in Responding to Catastrophic Cyber Risks ..... 12**
- Section 5: How Cyber Insurance Can Evolve to Respond to Catastrophic Risks ..... 14**
- Section 6: Key Takeaways of Catastrophic Cyber Risk..... 15**
- Acknowledgements ..... 16**
- About The Society of Actuaries Research Institute ..... 17**

# Strategies and Solutions Against Catastrophic Cyber Incidents

## An Expert Panel Discussion

### Executive Summary

This report addresses the evolving landscape of catastrophic cyber risks and the role of the cyber insurance sector in responding to these challenges. The goal of this comprehensive analysis is to explore the key issues, perspectives, and potential strategies for enhancing the effectiveness of cyber insurance in managing and mitigating catastrophic cyber risks. This report presents the findings of the fourth and final expert panel discussion focusing on catastrophic cyber incidents<sup>1</sup>.

This is the fourth and last report of a series of expert panel discussions focusing on catastrophic cyber incidents. In the first report, the definitions of catastrophic cyber risks were consolidated, mitigation strategies were examined, and specific challenges faced by the insurance industry were identified. The second report presented outcomes of a red teaming exercise simulating a catastrophic cyber incident in the transportation sector, exploring its impact on the insurance industry and economy. The third report summarized discussions on a scenario of a widespread cyber incident caused by a software supply chain vulnerability, affecting thousands of organizations globally.

In this expert panel meeting, the participants discussed various aspects related to catastrophic cyber risks and the role of the cyber insurance sector and its stakeholders in mitigating both pre-incident and post-incident challenges. They explored the actions that should be taken to address these risks and the role of the government in supporting the cyber insurance sector. The thresholds for intervention and the impacts of government action on the sector were also key topics of discussion. Additionally, the participants deliberated on the evolution of cyber insurance to better respond to catastrophic cyber risk events and highlighted key takeaways for actuaries and insurers from the discussions on this topic.

Building upon the comprehensive discussions held during the expert panel meeting, the following paragraphs summarize the key findings and insights derived from the exploration of catastrophic cyber risks and the role of the cyber insurance sector.

To begin, panelists engaged in a thorough discussion about the escalating threat landscape and emphasized the need for the cyber insurance sector to adapt rapidly to the growing magnitude and complexity of these risks. They recognized the systemic nature of catastrophic cyber risks and their potential wide-ranging impacts, underscoring the urgency for proactive measures and collaboration across industries to effectively address these risks.

Secondly, panelists delved into the challenges faced by the cyber insurance sector in responding to catastrophic cyber risks. They highlighted the limitations of traditional approaches and the need for continuous adjustments to underwriting standards and policies. The dynamic nature of cyber insurance was emphasized, with insurers issuing new coverage iterations every six months to keep pace with the evolving risk environment. This dynamism and

---

<sup>1</sup> The reports of the first three expert panel meetings are available at the Series web page [Catastrophic Cyber Risk: An Expert Panel Discussion Series | SOA](#)

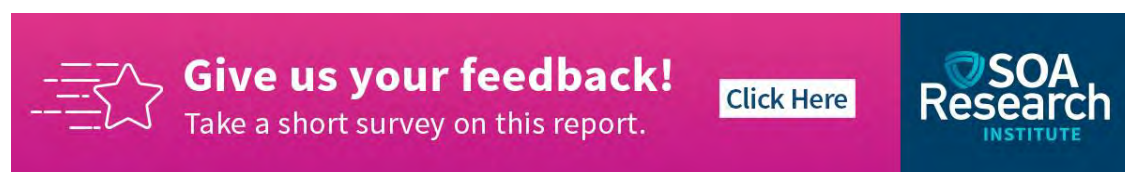
constant need for recalibration differs from some other areas of insurance and means some practices common elsewhere may not transfer cleanly to cyber insurance.

Next, panelists explored the potential role of government in supporting the cyber insurance sector. They discussed the importance of government intervention in addressing systemic challenges, enforcing regulations, and providing backstopping insurance. Finding the right balance between types of government involvement - enforcement, certification, and incentives - was deemed crucial to prevent overreach, while also ensuring the sector's stability and resilience.

Furthermore, panelists emphasized the necessity for the evolution of cyber insurance to effectively respond to catastrophic cyber risks. They discussed ongoing research activities aimed at understanding and quantifying the likelihood and impact of such events. The use of risk management platforms, new kinds of data, and evidence-based procedures to evaluate the effectiveness of controls and to guide risk mitigation efforts was also highlighted. The panelists stressed that cyber insurance is an ever-evolving field, adapting to the changing risk landscape and the varying profiles of insurers and policyholders.

Lastly, the key takeaways from the discussion revolved around the need for new models, organizations, and teams to navigate the challenges posed by catastrophic cyber risks. The absence of a universal definition for catastrophe was recognized, as it depends on the context and risk tolerance of each company. Panelists acknowledged the opportunity to collect more data and evaluate the effectiveness of controls, such as multi-factor authentication, in reducing cyber risk. They also suggested exploring the implementation of no-fault cyber insurance, which could provide opportunities for experimentation with federal incentives and thresholds for reimbursements.

In conclusion, this report underscores the critical need for the cyber insurance sector to evolve and adapt in response to the escalating threat of catastrophic cyber risks. It highlights the challenges faced by the sector and the potential role of government intervention. By embracing innovative strategies, proactive collaboration, ongoing research, and evidence-based approaches, the cyber insurance sector can enhance its effectiveness in managing and mitigating the impact of catastrophic cyber risks. This, in turn, will safeguard businesses, individuals, and public resources in an increasingly interconnected digital landscape.



A horizontal banner with a pink background on the left and a dark blue background on the right. On the left, there is a white star icon with horizontal lines extending from its left side. To the right of the star, the text "Give us your feedback!" is written in a bold, white, sans-serif font. Below this, in a smaller white font, is the text "Take a short survey on this report." To the right of this text is a white rectangular button with the text "Click Here" in a dark blue font. On the far right of the banner, the SOA Research Institute logo is displayed, featuring a blue shield icon with a white outline, followed by the text "SOA Research INSTITUTE" in white, with "INSTITUTE" in a smaller font size.

## Section 1: Background, Objectives, and Method

The purpose of this report is to present strategies and solutions for enhancing cyber resilience against catastrophic cyber events. These strategies and solutions are based on the findings of the first three meetings and subsequent reports, which were held to examine catastrophic cyber risks and conduct red teaming scenario analyses.

This report aims to provide a comprehensive and actionable plan that can be used by the cyber insurance sector and its stakeholders to strengthen their cyber risk management practices and increase their ability to respond effectively to catastrophic cyber events. It draws on the insights and recommendations generated during the expert panel meetings and distills them into a set of concrete and practical strategies that can be implemented at different levels of the cyber insurance sector and its stakeholders.

The report is intended for a wide audience, including cyber insurance companies, policymakers, regulators, industry associations, and other stakeholders who have a role to play in enhancing cyber resilience against catastrophic cyber events. Its ultimate goal is to promote a more proactive and collaborative approach to cyber risk management, one that recognizes the shared interests and responsibilities of all stakeholders and fosters greater trust and confidence in the cyber insurance sector as a key contributor to cyber resilience.

This report serves as the fourth and final installment of a series of expert panel discussions focusing on catastrophic cyber incidents.

Based on the October 2022 expert panel meeting, the first report<sup>2</sup> aimed to consolidate the definitions of catastrophic cyber risks, examine their mitigation strategies, and identify the specific challenges encountered by the insurance industry. Additionally, it laid the groundwork for the project's forthcoming red teaming exercises, establishing a framework for their implementation.

Derived from the January 2023 expert panel meeting, the second report<sup>3</sup> explored the outcomes of the initial red teaming exercise. This exercise simulated a catastrophic cyber incident targeting a critical infrastructure sector, specifically, the maritime transportation sector, and explored the subsequent repercussions on the insurance industry and the overall economy. The report included in-depth discussions on the coordinated cyber-attacks, in conjunction with a significant hurricane causing substantial disruptions to several major U.S. ports.

The third report<sup>4</sup> summarized the discussions of the March 2023 expert panel meeting where a red teaming exercise was conducted, and a widespread catastrophic cyber incident was taken into consideration. The incident was caused by a software supply chain vulnerability and had an impact on over three thousand organizations worldwide from different sectors.

Finally, this report is based on the May 2023 expert panel meeting where participants discussed the strategies and solutions to address catastrophic cyber risks. In support of this goal, the following research questions were provided to participants:

---

<sup>2</sup> Tatar, U., Nussbaum, B., Keskin, O. F., Dubois, E. V., & Foti, D. (2022). *Setting the Scene: Framing Catastrophic Cyber Risk An Expert Panel Discussion* (Catastrophic Cyber Risk: An Expert Panel Discussion Series). Society of Actuaries. <https://www.soa.org/resources/research-reports/2023/cat-cyber-risk/>

<sup>3</sup> Tatar, U., Nussbaum, B., Keskin, O. F., Clifford, D. C., Dubois, E. V., Foti, D., Bace, B., & Davis, R. (2023). *Red Teaming Analysis of a Catastrophic Cyber Attack on Critical Infrastructure An Expert Panel Discussion* (Catastrophic Cyber Risk: An Expert Panel Discussion Series). Society of Actuaries. <https://www.soa.org/resources/research-reports/2023/cat-cyber-risk/>

<sup>4</sup> Tatar, U., Nussbaum, B., Keskin, O. F., Clifford, D. C., Dubois, E. V., Foti, D., Bace, B., & Davis, R. (2023). *Red Teaming Analysis of a Widespread Catastrophic Cyber Incident An Expert Panel Discussion* (Catastrophic Cyber Risk: An Expert Panel Discussion Series). Society of Actuaries. <https://www.soa.org/resources/research-reports/2023/cat-cyber-risk/>



- What can the cyber insurance sector and its stakeholders do to mitigate the pre-incident challenges of catastrophic cyber risks?
- What can the cyber insurance sector and its stakeholders do to mitigate the post-incident challenges of catastrophic cyber risks?
- What should be the role of the government in supporting the cyber insurance sector to better respond to potential catastrophic cyber risk events?
- How would government actions impact the cyber insurance sector?
- How should cyber insurance evolve to better respond to catastrophic cyber risk events?
- What are the key takeaways for actuaries and insurers from these discussions on the topic of Catastrophic Cyber Risk?

The following sections of this report provide the outcomes of discussions of the expert panel, which was convened for a two-hour session to answer the questions above. To promote transparency and encourage candid discussions, participants were assured that no ideas were attributed to any individual or company in this report. Rather, the report's focus is on summarizing the ideas, opinions, and discussions shared during the panel session. However, the Acknowledgements Section includes the names of all participants who contributed to the discussion.

## Section 2: Pre-Incident Challenges of Catastrophic Cyber Risks

As cyber risks continue to grow in scale and complexity, the cyber insurance industry and its stakeholders are grappling with the challenge of mitigating the pre-incident challenges of catastrophic cyber risks. In response to this pressing issue, the initial question raised was, "What measures can the cyber insurance industry and its stakeholders take to address pre-incident challenges posed by catastrophic cyber risks?" Following this inquiry, a discussion ensued, which aimed to identify effective strategies and solutions for managing these risks and enhancing cyber resilience.

The first point the panel discussed regarded delineating the types of pre-incident strategies and solutions into one of two categories—mitigation or measurement of risk. One panelist started the discussion by emphasizing the meaning of the word "mitigate" in risk management, which typically means neutralizing a risk. However, other panelists argued that some risks cannot be completely neutralized, such as the lack of historical data or difficulties in modeling frequency or severity. The panelists suggested that underwriting and structuring coverage can help to mitigate such risks but cannot completely solve the problem. Another panelist pointed out that the use of the word "mitigate" was not necessarily about completely solving a problem but rather reducing the level of issues surrounding it. The panelists highlighted the importance of breaking down the list of challenges into specific categories and addressing each category separately. This approach can help identify the root causes of each challenge and provide more targeted solutions.

One of the key themes that emerged from the panel discussions was the importance of risk modeling in identifying potential risks and developing effective risk management strategies. Panelists suggested that risk managers should work to build more robust models, gather more data, and continuously refine their strategies to stay ahead of emerging risks. A major insurance firm performs both internal and external risk modeling. They use benchmarking to determine the types of limits that organizations qualify for, based on three factors: privacy, direct business interruption, and a ransomware exercise. Additionally, several companies are involved in security analytics, which enables firms to improve their security scores by making changes. The use of these tools has become increasingly popular in underwriting, even among traditional insurance companies. The panel also emphasized the importance of

collaboration between different stakeholders in the risk management process, including insurers, regulators, and policyholders, to ensure a more holistic and effective approach to managing risk. While risk modeling is a critical component of risk management, the panelists acknowledged that it is not foolproof and requires ongoing refinement and adaptation to stay ahead of emerging risks. The panelists touched on the topic of insurable versus uninsurable risks and suggested that the insurance industry needs to take a more nuanced approach to cyber risk coverage, rather than treating all cyber risks as uninsurable.

Another key theme is mitigation practices, or more specifically pre-incident services or controls to limit exposure and heighten defenses. Panelists agreed that there was no magic bullet solution to mitigate pre-incident challenges and that it would require an aggregate of many solutions. Multiple panelists agreed that better employee training is necessary to mitigate or prevent incidents. The quality and effectiveness of the employee training has to be improved to address this issue. They recommended at least one provider of user training that was seen as effective.<sup>5</sup> One panelist noted that business email compromise is becoming more impactful than ransomware, emphasizing the importance of cybersecurity awareness across the workforce. It is crucial for the C-suite to be fully engaged in this process, encouraging multiple trainings each year and adhering to all cybersecurity controls, as they handle the most sensitive data. Further, one panelist proposed systematic threat hunts to strengthen security visibility. Specifically, they referenced Neighborhood Keeper, a free and anonymous threat detection and shared intelligence program for industrial control systems security that is sponsored by the Department of Energy<sup>6</sup>. The program helps small or large critical infrastructure players share threat intelligence with a low-cost device without revealing any sensitive information about the participant infrastructure and facilitates direct communication between participants and partners such as the Electricity Information Sharing and Analysis Center (E-ISAC).<sup>7</sup> There is a mutual economic benefit in the Neighborhood Keeper Program. Dragos, which must pay to maintain the infrastructure, gets access to data in aggregate to monitor emerging threat techniques and procedures - which improves their product lines. At the same time, the individual companies get basic monitoring capabilities. Insurance sector complains about lack of data, perhaps they should consider better incentives to gather real-time data at scale by providing data gathering processes that actually provide a benefit other than only premium reduction.

Moving on to another important facet of the problem, the panelists also delved into the insurability of cyber risks and the role insurers can play in promoting good cyber hygiene and incentivizing cyber risk controls. The panelists asserted that addressing risks largely depends on whether or not it is an insurable or uninsurable catastrophe. This helps determine whether or not the insurers attempt to limit their own exposure to cyber risk or if they will limit the impacts of cyber risk on the overall economy. Attempts at limiting overall risk are largely done through the creation of incentives around adding certain controls, such as requiring companies to adopt certain cybersecurity practices. For example, a company could be required to have encrypted backups with the ability to deploy them within 24 hours. This is a high bar for medium- and small-sized companies, but it creates incentives for SMEs while also insulating cyber insurance providers from the impacts of cyber events. However, they also acknowledged that this could be a long and expensive process and could be difficult for smaller businesses to implement. Moreover, such controls will only help against specific threat vectors, and modern cybersecurity will always require defense-in-depth.

The participants discussed how adopting certain controls can help push buyers to make cyber risks more insurable. Marsh was mentioned in the discussion, as they had released a list of twelve key controls that they recommended policyholders implement last year. Despite a slight softening of the market, insurers will still provide coverage

---

<sup>5</sup> <https://www.knowbe4.com/>

<sup>6</sup> <https://www.dragos.com/resource/department-of-energy-doe-announces-funding-award-for-dragos-neighborhood-keeper-program-for-threat-detection-and-shared-threat-intelligence-across-small-infrastructure-pro/>

<sup>7</sup> <https://www.dragos.com/neighborhood-keeper/>



before the implementation of the controls, but they will sub-limit until the control is attested to. The government has played an important role in promoting multi-factor authentication (MFA) as a critical control to improve cybersecurity, making cyber risks more insurable. The insurance sector has also played a vital role in making this possible. The participants then explored what can be done to make cyber risks more insurable, including collaborating with other stakeholders. From an academic perspective, the extreme value theory can be used to model catastrophic events, and financial tools may be used to address them to some extent.

The panelists also explored the use of financial products in managing catastrophic cyber risks, such as CAT bonds<sup>8</sup>. While these instruments can provide a backstop in the event of a catastrophic cyber event, the speakers noted that their impacts are not always obvious, and companies may reduce their underwriting standards as a result of having such a backstop. One panelist suggests that interest rates may need to go up to address this issue. This could actually increase the likelihood of claims and higher loss ratios, highlighting the need for caution when using financial products to manage risk.

The discussion then moved toward the monoculture and concentration of IT infrastructure. With many companies reliant on the same infrastructure, even those who possess good cyber hygiene can be impacted if a cloud provider or other such component is attacked. This shared infrastructure reliance, particularly on cloud computing, introduces a new realm of potentially catastrophic risk. There is little that can be done to mitigate this type of risk for SMEs in particular. This shared infrastructure risk is one area in which it may be possible to make improvements and for the government or insurance sector to push for systemic risk reduction. Shared infrastructure usually comes with a shared responsibility. For example, in Amazon Web Services' (AWS) approach, AWS provide a way to get automated reports from their side through service documentation, 3rd party attestation documents, and audit reports that are relevant to the clients' services. This would result in a new "transparency model" that insurers are not used to because it would require building a cyber case that goes beyond questionnaires and single player security audits.

The discussion also delved into emerging technologies such as Artificial Intelligence (AI) and their potential to automate controls for cyber underwriting and pricing. While these technologies could potentially make cyber risks more insurable and lead to more accurate pricing, the speakers noted that small to medium businesses may not have the personnel or expertise to implement such controls, making automation an unattractive option. The idea that the utility of blockchain could be set up to substantiate risk controls, validate in real-time, and create a predictive model has become increasingly popular in recent years, necessitating a review of cyber risk and AI. The experts agreed that AI is complex and that there are a few key questions that must be answered from an insurance perspective: namely "Who owns the AI" and "What do you mean by AI?". AI can be developed by a multitude of actors, such as third parties, big data, or one's own company. Knowing who owns the AI will inform insurers' decision-making in terms of liability. Secondly, there are numerous different types and uses of AI. Insurers will need to know where it is residing and if it is used to mitigate, identify, or measure risk.

How adversaries may use this technology is also a concern, as it is almost certain that malicious actors will leverage AI to conduct cyberattacks in the future. However, it is unlikely that companies will be overrun with such attacks. The market incentives for developing defenses that can stand against AI- and for defenses that leverage it- are high enough that defensive development will not necessarily lag. The panelists agree that the potential of AI in security is not yet fully understood, but security technologies must improve to keep pace with evolving hacking techniques. In practice, cyber threat actors have demonstrated the ability to bypass endpoint detection systems that leverage

---

<sup>8</sup> A catastrophe bond (CAT) is a high-yield debt instrument used to raise funds for insurance companies to be prepared against catastrophic incidents, such as a natural disaster. In case of a qualifying incident, the issuer is eligible to receive funding from the bond. In case that the insurance company receive funds, the interest and repaying the principal can be deferred or exonerated. (<https://www.investopedia.com/terms/c/catastrophebond.asp>)

machine learning. One panelist added to this point, citing their experience with AI-based technologies. They noted how fragile these systems are and that it is very much a "garbage-in, garbage-out" system. Moreover, AI systems can also be perfect-in-garbage-out due to the obscure way that "creativity - the novel methods use to fragment and recombine solutions". The result is that AI regularly hallucinates, even with verifiable inputs. While the panelists are a big proponent of using these tools, they would not suggest doubling down on an AI-backed mechanism alone.

Finally, the panelists discussed the need for effective risk management in the insurance sector and highlighted the importance of trust in lawyers to deal with cyber incidents. However, they also noted that cybersecurity risk management is not as comprehensive as the technical incident planning that actually happens, indicating that there is room for improvement in this area. One panelist mentions the importance of having a well-documented incident response plan in place, as the current plans often fall solely on lawyers to develop and implement. Other panelists agree with this sentiment, adding that the insurance sector needs to take a more proactive approach to catastrophic cyber risk. They mention Lloyd's and their realistic disaster scenario modeling, which requires some of their syndicates to undergo rigorous cybersecurity risk management measures. However, the panelists note that there is currently no comparable approach outside of Lloyd's, emphasizing the need for the insurance industry to come together and address this issue collectively. This is an example of where sector-level coordination of existing best practices and approaches could reduce collective risk.

The panelists also remarked on how insurance is not necessarily about *not* taking on risks but about getting fairly compensated for doing so. Larger risks will be taken on, as long as there is money to be made and enough capital to ensure the insurer remains solvent. Insurers also follow the law of large numbers, meaning that "the premiums of the many pay for the losses of the few." When an individual account is underwritten, the actuaries and underwriters evaluate what kind of capacity, terms, and conditions can be outsourced and how much should be paid for each based on expectations for cyber-attack frequency and severity. One specific issue regarding insurer costs is class action lawsuits arising from cyber breaches or unintended disclosure of sensitive information. For actuaries and underwriters, the main concern is what the courts or legal system will allow for in the pursuit of these privacy injury cases. These lawsuits have greatly contributed to the overall loss picture and represent one of the largest challenges when it comes to cyber insurance. The panelists conclude by suggesting that while the government may not be the best entity to lead the effort toward mitigating catastrophic cyber risks, state regulators and other industry watchdogs could take a more active role in promoting effective cybersecurity risk management practices in the insurance sector.

### Section 3: Post-Incident Challenges of Catastrophic Cyber Risks

As cyber threats continue to evolve and become more sophisticated, the risk of catastrophic cyber events and their aftermath looms large for organizations and society as a whole. In this context, cyber insurance has emerged as a key tool for managing cyber risks and mitigating their impacts. However, as the frequency and severity of cyber incidents increase, the focus is shifting from pre-incident risk mitigation to post-incident response and recovery. This raises the question: What can the cyber insurance sector and its stakeholders do to mitigate the post-incident challenges of catastrophic cyber risks? In the discussion, we explore this critical issue and examine strategies and solutions for enhancing cyber resilience in the aftermath of a catastrophic cyber event.

During the discussions, panelists found themselves once again deliberating over the definition of catastrophe and the feasibility of preparation for such a dire situation. An instance cited was that an attack on 30-50 companies may not constitute a catastrophe, whereas an attack on 50% of hospitals or water systems would. The concept of catastrophe appears to hinge partially on the sector or industry being targeted.

As the discussion continued, a possible exacerbating factor of a catastrophic cyber event would be the unavailability of reinsurers in the aftermath. As primary insurers heavily rely on the reinsurance market, with only a handful of

carriers providing capital for numerous cyber insurance carriers, the withdrawal of just one reinsurer's coverage could pose a significant challenge for the entire market. This issue is further compounded by reinsurers already cutting back coverage due to climate change (another example of a set of hazards where frequency and severity are increasing and causing greater losses).

The panelists also discussed the impact of significant vulnerabilities, such as Log4j, on the insurance market. One of the panelists suggests one way of improving the response of insurance companies to the discovery of such vulnerabilities was to invite them to participate in the information sharing initiatives of National Institute of Standards and Technology (NIST). This would enable insurers to become aware of disclosed vulnerabilities at the same time as others. In addition to the NIST's National Vulnerability Database, Joint Cyber Defense Collaborative (JCDC) by Cybersecurity and Infrastructure Security Agency (CISA) runs various operational coordination programs for incident coordination and response. Software Engineering Institute (SEI) provides a Coordinated Vulnerability Disclosure Program that control information under embargo before a public disclosure to the NIST NVD. KraftCERT (Norweigh) provides similar services for Nordic critical infrastructure to both the SEI coordinated disclosure and the JCDC operational collaboration. Germany is trying to promote Common Security Advisory Framework (CSAF) and related standards for improving the ability to automate many of these processes without the need for centralized systems managed by coordinators.

One panelist expressed how they believe the industry needs to be better at lobbying state governments and federal regulatory agencies to hold businesses accountable and avoid class-action lawsuits. Even companies following all the currently recommended best practices can become victims of a cyberattack through mechanisms like zero-days or supply chain compromises. The commonplace villainization of these companies in the media and high losses to class action lawsuits indicate a need for significant revision to what is considered privacy in the U.S. Not only is this type of fierce litigation not seen anywhere else in the world, but the U.S.'s approach to privacy also prevents companies from effectively reducing their cyber risks. The panelists note that cultural factors in the U.S. make it more likely for businesses to be sued following a cyberattack. This can be a significant financial burden for organizations, particularly small and medium-sized businesses that may not have the resources to defend against lawsuits. Fear of breaching privacy laws and consequential litigation, for example, has pushed victims to avoid inter-organizational cooperation.

The conversation also touched on the limitations of information sharing among companies after an incident. The panelists noted that many companies may be reluctant to share their own incidents and vulnerabilities due to concerns about privacy and confidentiality. A lack of information sharing means that industry partners may not receive the crucial information they need to avoid falling victim to similar attacks. This phenomenon has been seen in practice by one panelist within the Space Information Sharing and Analysis Center (ISAC). The panelist attests that the Space ISAC has not actually facilitated the flow of information about specific breaches amongst member organizations, who instead tend to conduct joint open-source intelligence work. It is clear that these organizations have their own intelligence, but the aforementioned fear of litigation means that the ISAC has turned into a conduit of government-industry exchange rather than an inter-industry exchange. This is true for most ISACs. For example, Water ISAC provides incident summaries (from member submissions) but does not coordinate flows of information during release. However, some others such as Defense Industrial Base (DIB) ISAC has performed these processes of connecting companies. KraftCERT (Norweigh) has also performed this coordination function as well. Panelists suggest that sharing information is crucial for everyone's benefit so that lessons can be learned, and future incidents can be prevented. To address this challenge, the speakers suggest the need for incentives, such as rewards or incentive-based systems, to encourage companies to share their information more freely. For example, one panelist mentions the insurance industry's creation of organizations that encourage its members to share incident data, where members who share more information can receive access to more shared data is beneficial. This sort of rewards-based system could be an effective way to encourage companies to share their information while maintaining their privacy and confidentiality. Such a system would require a secure infrastructure that can be

audited by the participating companies. Or they would need to set up a system like Dragos/DOE Neighborhood Keeper where the clients can only query the system but cannot actually obtain any data where the query is performed in a way that it formally verifies that no data can be released.

It is worth noting, however, that the success of such incentive systems may depend on the size and makeup of the industry in question. For example, the speakers note that the space sector may be particularly hesitant to share information due to the sensitivity of some of the data involved. Thus, while rewards-based systems may be useful for some industries, they may not be universally applicable. Ultimately, the success of any information-sharing initiative will depend on the willingness of individual companies to share their data, as well as the effectiveness of the platform itself in protecting the privacy and confidentiality of that data. However, the panelists agree that blanket immunity is also not the answer. Such a solution would be unfair, as there are some companies that exhibit gross negligence and should be penalized. A model worth considering to address this issue might be the no-fault insurance model, which is an alternate model in the insurance industry. For example, for auto insurance, this is organized at the state level in which every entity must be insured, pay in, and give up the right to sue. For the public interest, if this is applied to some organizations in cyber insurance, this could provide a way to circumvent liability issues and alleviate the fears of information sharing, which may in turn lead to increased cyber preparedness.

The panelists delved into the details of the new cyber catastrophe (CAT) bond by Beazley, which is a specialty insurer and reinsurer. Being the first<sup>9</sup> CAT bond in cyber insurance is a significant development in the insurance industry. This bond, launched in January 2023, is an Insurance-Linked Security (ILS) instrument specifically designed for catastrophic cyber and systemic events. What makes this bond so unique is that it is liquid, which means that it can be bought and sold easily on financial markets. The bond provides protection to Beazley in case of a catastrophic event, with coverage up to \$300 million. Panelists note that the creation of this bond could signal a shift in the industry towards more innovative and tailored solutions for insuring against cyber risks.

## Section 4: The Role of Government in Responding to Catastrophic Cyber Risks

As the threat of catastrophic cyber risks continues to increase, the role of the government in supporting the cyber insurance sector has become a critical issue. While the cyber insurance sector plays a vital role in managing cyber risks and mitigating their impacts, there are limits to what it can achieve on its own. Government intervention may be necessary to address the systemic challenges posed by catastrophic cyber risks and enhance cyber resilience. The discussion explores the question “What should be the role of the government in supporting the cyber insurance sector to better respond to potential catastrophic cyber risk events?”

In the conversation, the panelists discuss the topic of insurance and risk management and the role of government from various perspectives. They touch on different types of insurance policies such as no-fault insurance, workers' compensation insurance, and cyber insurance, and the need for government regulation in these areas. They also discuss the challenges associated with insuring against catastrophic cyber risk events and the potential role of the federal government in providing backstopping insurance.

The first point the panel discussed was the idea of government involvement in enforcing and regulating cybersecurity measures. Such regulation would be analogous to that seen with workers' compensation/OSHA and auto liability mechanisms like licenses and registrations. Both of these examples of government regulations stem from the fact that the associated risk arenas affect the whole economy and population broadly. Cyber risk is undoubtedly another form of endemic risk that falls within this category, suggesting that it would be appropriate for

---

<sup>9</sup> <https://www.ft.com/content/a945d290-a7f1-427c-84a6-b0b0574f7376>

similar controls to be put in place. Any regulations, however, must require some form of enforceability (or “teeth”) and a model for certification and incentives. Without these caveats, regulations become “just another pile of paper.” The panelists did emphasize, however, that they were not advocating for government overreach; rather, they were developing a solution based on the idea that the government would likely intervene anyway.

One of the key points discussed is the importance of insurance as a means of protecting businesses, individuals, and public resources. Workers' compensation insurance and no-fault auto insurance are highlighted as examples of insurance policies that protect businesses from potential legal battles resulting from accidents involving their employees or vehicles. Workers who are injured in accidents require medical attention and rehabilitation, which can be expensive for businesses to cover without insurance. However, by having workers' compensation insurance, businesses can protect themselves from costly legal battles and provide necessary care for their employees. On the other hand, the panelist emphasized the importance of everyone being insured as part of the quid pro quo of workers' compensation insurance and no-fault auto insurance. This means that for businesses to benefit from these types of insurance, everyone involved must be insured, including employees and drivers. One speaker likened this requirement to the concept of having car insurance before being allowed to drive, stating that businesses should also be required to have their systems insured in order to conduct business over the Internet. Both auto liability and workers' compensation are risk areas that affect the whole economy and population broadly, as does cyber risk.

In these analogies, one panelist equated the internet to a public resource like public roads, which is commonly referred to as the “information superhighway”. Just as drivers are required to have car insurance to use public roads, businesses should be required to have insurance to use the Internet. If a company wants to be on the internet and on the “internet superhighway,” they must be insured and meet certain underwriting criteria, preventive measures, financial controls, and other such necessities. In return, they are protected from unlimited liability. The panelist notes that this could be a potential model for regulating businesses that conduct business online, although they do not necessarily advocate for it.

The conversation also touched on the practicality and effectiveness of no-fault insurance in various scenarios, particularly for larger risks such as cyber insurance. One of the panelists mentioned that people who opt for no-fault insurance may end up paying higher premiums, around 30 to 50% more than traditional insurance policies. However, the benefit of no-fault insurance is that it solves the problem of everyone being insured and increases the pool of insured individuals, which can limit liability. The speakers then delved into the application of no-fault insurance in the context of larger companies that have several hundred-million-dollar towers and policies for cyber insurance. The conversation shifted to whether the concept of no-fault insurance still holds for bigger risks, and whether there is an excess in workers' compensation.

The panelists acknowledged that these types of government-backed mechanisms would have to be passed by state legislatures, pursuant to the Ferguson Act. This could be difficult to achieve, as this requires legislators that understand the risk landscape and the appropriate controls needed to address this risk. Currently, insurance is state-regulated but could be amended at the federal level by changing the McCarran-Ferguson Act. The panelists suggested that the government could step in and create more responsibility from a regulatory perspective not only around HIPAA but also other regulatory frameworks.

Another suggested option was to build up discussions with clients about benchmarking and limit profiles. Definitionally, benchmarking is based on what others have already done or tools they have bought, while data loss is predicated on public historical loss figures. Both of these tools necessarily use backward-looking data sets that can be used to estimate future losses. This must be done while also considering specific company growth trajectories in order to best determine how to build an insurance policy that anticipates where a company will be if/when a loss occurs.

The conversation then moved on to a recent government announcement that holds software companies liable for vulnerabilities in their software that lead to harm to users. The panelists discussed the impact of this announcement on cyber insurance. They speculated on potential solutions for holding software companies liable for vulnerabilities in their software that lead to harm to users, including the possibility of a certification process. This software could potentially be certified in an unbiased lab, but putting this into practice would be extremely difficult. Every possible flaw in one company's software permeates deep into the interconnected supply chain, making the assignment of liability difficult and potentially catastrophic for software owners.

Lastly, the panel explored the topic of federal backstopping. They reiterated that if most of the problems arising for companies are liability-related, then no-fault insurance would be the best option. A backstop would only come into play if there were no no-fault mechanism in place and large losses are incurred from class action lawsuits. The panelists went on to say that if the federal government were to provide backstopping, the question then becomes who benefits from these class-action lawsuits. Is it the plaintiffs, or is it the lawyers who are bringing the lawsuits? One panelist suggested that the federal government could require that the lawyers be paid a fee based on a percentage of the actual loss suffered, rather than the full amount claimed in the lawsuit. This would discourage frivolous lawsuits and would also ensure that the plaintiffs receive a fair settlement.

The panelists discussed the government's role in providing a public-private partnership to address the growing protection gap due to the increased use of war exclusions. They debated the possibility of a federal backstop or "backstop+" program in which the government would cover certain industries or risks. Some believed that implementing cyber hygiene measures could make the private market more comfortable offering higher limits, while others were skeptical that it would require more government funding than they are willing to spend.

From the federal perspective, it is important to focus on first-party losses that are immediately incurred following a cyberattack or another event. Large first-party losses incurred following an act of terrorism, for example, are covered under the Terrorism Risk Insurance Act (TRIA). TRIA was set up after 9/11 after a meeting between the federal government and several larger insurance carriers who decided what losses the insurance industry would not cover. This decision was made with the understanding that the industry could not sustain itself if another catastrophic event were to occur in a short time frame. The uninsurable losses that insurance companies could not cover while still offering affordable premiums were then backstopped with TRIA. While TRIA focuses on catastrophic risk in terms of terrorism, it nonetheless offers some insight into how a federal backstop for catastrophic cyber risk could function. Finally, a speaker mentioned that in order to maintain an A+ or better financial rating from AM Best, insurers must be prepared for two very large catastrophes occurring in a short period of time.

## Section 5: How Cyber Insurance Can Evolve to Respond to Catastrophic Risks

As the threat landscape of cyber risks continues to expand, the cyber insurance sector faces the challenge of evolving to better respond to catastrophic cyber risk events. The traditional approach to cyber insurance may no longer be sufficient in a world where the magnitude and complexity of cyber threats are growing rapidly. Therefore, the question of "how cyber insurance should evolve to better respond to catastrophic cyber risk events" has become critical. In the final question, we explore the key issues and challenges involved in the evolution of cyber insurance and examine potential strategies and solutions for enhancing its effectiveness in managing cyber risks and mitigating their impacts.

The panelists began this section of the discussion by remarking on how cyber insurance has been growing both in popularity and in the staggering amount of capital entering the industry. As a whole, cyber insurance has been bought, adopted, and grown tremendously over the past few years. Over the last three years, underwriting companies have been adjusting their underwriting standards and policies to react to the market's shifting nature, especially in response to ransomware exploding in part as a result of the growth of remote work during COVID-19.



Carriers were issuing new policy coverage iterations every six months, demonstrating the dynamic nature of cyber insurance. One panelist pointed out that cyber insurance has been the least static mode of insurance for the last five years, meaning it is constantly evolving to adapt to the changing risk environment.

The panelists believe that cyber insurance will continue to change and adapt as the risk environment evolves. One panelist suggested that there may be more or fewer exclusions in cyber insurance policies, depending on each underwriter's evaluation of what they can hold on to their balance sheet from a risk perspective. Cyber risk management is also not monolithic, with a plethora of companies in this space of different sizes, structures, and risk appetites. The decision of whether to include or exclude more or less will depend upon the profile of the particular insurer, who they are insuring, and the overall cyber risk landscape.

The panelists also discussed ongoing research activities for cyber risk pricing and making references and guidelines available to reduce risk levels. They agreed that it is important to put more effort into determining the likelihood and impact of a catastrophic cyber event, noting how employing a good modeling tool could help guide and predict events.

One mechanism already used to improve responses to cyber risk events includes risk management platforms. These tools are used to provide clients with a list of specific vendors and products that aid in risk mitigation. Risk management platforms are generally only made available to mid-sized companies where more support is needed, as larger companies often possess their own risk management schema.

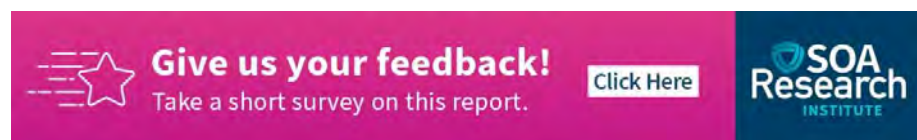
## Section 6: Key Takeaways of Catastrophic Cyber Risk

The panelists agreed that the industry is going to need new models, organizations, teams, and an understanding of how to define catastrophe. A universal definition is difficult to conceptualize because it largely depends on context—a catastrophe for one company will not be the same as another's. Some individuals may define it as the level of risk beyond which the industry or company would not be willing to take that risk. This definition is similar to the one utilized at the federal level, which views a catastrophe as the level above which the insurance market would no longer be able to take on that risk. The question then becomes “How much is too much for the insurance industry?” This could be the point at which a federal backstop would step in.

Cybersecurity may also not need to be its own separate category of risk. It may be useful to consider this type of risk in terms of the actual event as well as the mechanics of that peril. This could aid in dispelling the confusion that comes with dichotomizing cyber against the other types of risk.

There has also been progress in focusing on certain controls, including taking a harder line and requirements for baseline controls like MFA. The panelists agreed that the insurance industry should capitalize on the opportunity to collect more data to evaluate the ecosystem and the effectiveness of these controls compared to the risk landscape. Implementing more evidence-based procedures allows for the creation of guidelines that detail what the next steps/controls should be. This is much more effective at mitigating cyber risk than simply ordering certain companies to adopt controls without an empirical basis.

One of the key takeaways regarding which methods can be used to reduce losses and risk levels is that no-fault cyber insurance is the best option. There will be initial challenges, but there are many opportunities for experimentation with federal incentives and thresholds for reimbursements.



## Acknowledgements

The authors' deepest gratitude goes to those without whose efforts this project could not have come to fruition: the volunteers who generously shared their wisdom, insights, advice, guidance, and arm's-length review of this study prior to publication. Any opinions expressed may not reflect their opinions nor those of their employers. Any errors belong to the authors alone.

### Expert Panel Participants:

Michael Bean, Canadian Institute of Actuaries

Nicole Becher, Google

Kenneth Crowther, Xylem

Greg Falco, Johns Hopkins University

Ben Goodman, CyRisk & 4A Security and Compliance

Tyler Moore, University of Tulsa

Norman Niemi, American Academy of Actuaries

Reid Putnam, Gregory & Appel Insurance

Sasha Romanosky, RAND Corporation

Marc Schein, Marsh McLennan

Jeremy Straub, North Dakota State University

Maochao Xu, Illinois State University

### At the Society of Actuaries Research Institute:

Rob Montgomery, ASA, MAAA, FLMI, Consultant -Research Project Manager

### Facilitators at the University at Albany:

Unal Tatar, PhD

Brian Nussbaum, PhD

Omer F. Keskin, PhD

Elisabeth Dubois, MBA, PMP

Dominick Foti, MBA

Brianna Bace

Rian Davis

The Society of Actuaries Research Institute would like to acknowledge the generous contribution of the Casualty Actuarial Society to the funding of this research.

## About The Society of Actuaries Research Institute

Serving as the research arm of the Society of Actuaries (SOA), the SOA Research Institute provides objective, data-driven research bringing together tried and true practices and future-focused approaches to address societal challenges and your business needs. The Institute provides trusted knowledge, extensive experience and new technologies to help effectively identify, predict and manage risks.

Representing the thousands of actuaries who help conduct critical research, the SOA Research Institute provides clarity and solutions on risks and societal challenges. The Institute connects actuaries, academics, employers, the insurance industry, regulators, research partners, foundations and research institutions, sponsors and non-governmental organizations, building an effective network which provides support, knowledge and expertise regarding the management of risk to benefit the industry and the public.

Managed by experienced actuaries and research experts from a broad range of industries, the SOA Research Institute creates, funds, develops and distributes research to elevate actuaries as leaders in measuring and managing risk. These efforts include studies, essay collections, webcasts, research papers, survey reports, and original research on topics impacting society.

Harnessing its peer-reviewed research, leading-edge technologies, new data tools and innovative practices, the Institute seeks to understand the underlying causes of risk and the possible outcomes. The Institute develops objective research spanning a variety of topics with its [strategic research programs](#): aging and retirement; actuarial innovation and technology; mortality and longevity; diversity, equity and inclusion; health care cost trends; and catastrophe and climate risk. The Institute has a large volume of [topical research available](#), including an expanding collection of international and market-specific research, experience studies, models and timely research.

Society of Actuaries Research Institute  
475 N. Martingale Road, Suite 600  
Schaumburg, Illinois 60173  
[www.SOA.org](http://www.SOA.org)