Setting the Scene: Framing Catastrophic Cyber Risk An Expert Panel Discussion

Catastrophe and Climate

PART 1

JANUARY | 2023

SOA Research INSTITUTE

Setting the Scene: Framing Catastrophic Cyber Risk

An Expert Panel Discussion

AUTHORS Unal Tatar, PhD
Brian Nussbaum, PhD
Omer F. Keskin, PhD
Elisabeth Dubois, MBA, PMP
Dominick Foti, MBA

SPONSOR Catastrophe and Climate Strategic Research Program Steering Committee

Casualty Actuarial Society

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.

CONTENTS

Setting the Scene: Framing Catastrophic Cyber Risk

An Expert Panel Discussion

Executive Summary

With the growing threat of cyber incidents, organizations and governments are rightfully concerned. In recent years, cyber incidents have caused significant losses to entities and insurers across the world. The threat of a Catastrophic Cyber risk is ever looming. Therefore, there is a need to understand and provide greater context around the topic of catastrophic cyber risk, which has implications for insurance companies, reinsurers, regulators, consumers, and society.

Taking a multi-disciplinary, holistic approach to catastrophic cyber risk, we conducted an expert panel study. The panelists brought an array of experiences and backgrounds, creating a strong and diverse conversation on catastrophic cyber risk. This is the first of four expert panels and subsequent reports in this series.

The objectives of this panel discussion were to:

- Elicit and synthesize insights from experts on framing catastrophic cyber risks, available tools and methods to address these risks, and challenges,
- Further, develop an outline for future red teaming exercises and improve the understanding of defining catastrophic cyber risk, how catastrophic risks are handled, and catastrophic cyber risk scenarios.

The goal of the discussion was not to reach a consensus but seek and identify all interpretations in the areas of interest. Therefore, many of the comments made and claims are not attributed to all participants. The discussion focused on three specific areas, including defining catastrophic cyber risk, how said risks are handled, and catastrophic cyber risk scenarios.

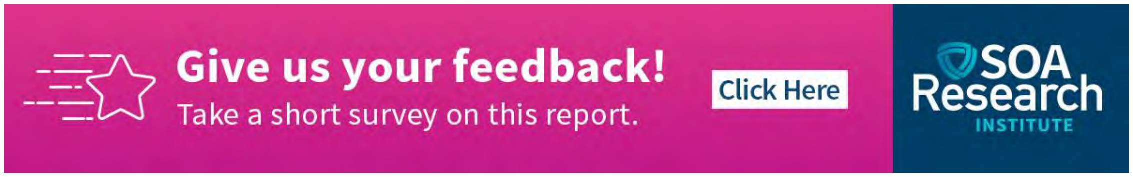
To begin, panelists discussed several definitions of catastrophic cyber risk, emphasizing there is no one size fits all solution. Panelists share that understanding catastrophic cyber risks are critical since it is challenging to calculate the likelihood and consequences as opposed to traditional risk events faced by insurance companies, as such risks may impact multiple interdependent sectors, with a large number of insured entities being affected at one time. Attacks do not have geographic borders, and the impact and frequency of the risks may be unknown. At the forefront, catastrophic cyber risks are seen as a risk that impacts the **quality of life for a large number of people, impacts the confidentially, integrity, and availability of information, or causes a wide-scale business interruption.** Unlike the more human-centered definitions, though, it is stipulated that catastrophic cyber risk for the insurance industry is based on the financial impact and potential data loss.

Second, the panel sought to discuss how catastrophic cyber risks are handled. Here several tools, techniques, and data sources are discussed in their relation to catastrophic cyber risks. The panelists share that to evaluate cyber risks, insurers use firmographics, historical incident claims data, technographics, and cyber modeling. Despite the several techniques discussed, the changing insurance marketplace presents challenges, primarily with the evolution of ransomware.

Next, panelists discussed catastrophic cyber risk scenarios that would help model the areas of the unknown in the industry. There was a discussion on sector-specific and critical infrastructure (CI) cyber risk events, where attacks on CI were of grave concern to panelists, both from a public good and insurance perspective.

Finally, major challenges were seen in how cyber incidents are handled. Said challenges exist in sparse cyber data and modeling frequency of catastrophic risks. Likewise, communication, digital forensics, and scalable responses are problematic in responding to cyber incidents.

The remainder of this document provides further details of the panel's discussion on these topics.



Background, Objectives, and Method

Increasing rates of cyber incidents, the systemic nature of cyber weaknesses, and emergent cyber threats have become significant concerns for organizations, governments, and the insurance sector. The growing catastrophic risks that an entire town, country, or even world may face due to cyber attacks or systemic vulnerabilities can severely impact technological infrastructure, public health and safety, economic security, and political stability. In recent years, cyber incidents have caused significant losses for insurance carriers and buyers of insurance, triggering a hard cyber market. The need to understand and prepare for catastrophic cyber risks is an evolving challenge with relevance to insurance companies, reinsurers, regulators, consumers, and society.

Cyber risk requires a multi-disciplinary approach, consisting of professionals across sectors and specialties. On October 28, 2022, the University at Albany research team, with the support of the Society of Actuaries (SOA) Research Institute, assembled an expert panel to discuss catastrophic cyber risk. This report serves as the deliverable of the first panel in a series of four, where future panels will use the feedback from experts to create and elicit information via red teaming[1] scenarios and in-depth discussions. Each participant who volunteered to be a part of the discussion was selected because of their professional or academic responsibilities in cybersecurity or risk management in an actuarial or insurance context. The group was diverse in terms of employment, including private and public sector from actuaries, academics from an array of backgrounds, engineers, computer scientists, and risk managers from various kinds of firms. Fourteen panelists participated, representing actuarial sciences, the insurance industry, the risk management domain, the cybersecurity domain, and academia.

The panel discussion was conducted in three sections on Zoom. For Sections 1 and 2, participants were broken into three groups which were sent to breakout rooms to discuss the questions at hand within smaller groups. For the final section, panelists participated in a plenary session.

The objectives of this panel discussion were to:

- Elicit and synthesize insights from experts on framing catastrophic cyber risks, available tools and methods to address these risks, and challenges
- Further, develop an outline for future red teaming exercises and improve the understanding of defining catastrophic cyber risk, how catastrophic risks are handled, and catastrophic cyber risk scenarios.

This document summarizes the discussion that occurred during the three-hour expert panel. To encourage openness during the discussion, the facilitators assured the participants that this report would not attribute comments to individuals or companies, so no names appear in the body of the report. The names of those who participated are included at the end of the report. The expert panel sought to identify various opinions in the areas of interest, not simply reach a consensus. This document is a summation of the comments made by participants and cannot be attributed to all participants.

[1] Red teaming is defined as "the simulation of adversary decisions or behaviors, where outputs are measured and utilized for the purpose of informing or improving defensive capabilities". More information on red teaming can be found at: https://www.albany.edu/sites/default/files/2019-11/CART%20Definition.pdf

Section 1: Understanding Catastrophic Cyber Risk

Before starting the discussion, the panelists were split into three groups, placed in breakout rooms, and asked to discuss two general questions: How do we define catastrophic cyber risks? and What is a catastrophic cyber risk for the insurance industry? The insights from the panel discussions are given below.

1.1 DEFINING CATASTROPHIC CYBER RISK

Definitions of catastrophic risk varied significantly throughout the discussion. Participants agreed that many agencies and organizations seek to define what makes up a cyber catastrophe but are faced with varying degrees of success. As one participant stated, it is clear that how we define catastrophic cyber risk is "in the eye of the beholder." Catastrophic cyber risk can be seen differently from everyone's point of view, where there is no black or white. In this, there are lots of gray areas of what a catastrophe risk is. Yet throughout almost all the definitions, widescale attacks on critical infrastructures (e.g., energy, transportation, and healthcare) are deemed catastrophic.

Definitions of catastrophic cyber risk can be taken from how catastrophic risk is defined in the physical world. From a standard insurance perspective, catastrophic risk is typically defined as a single event exceeding a certain amount in insurable losses or a certain number of affected insurers. Although catastrophic cyber risks can be defined the same way, we have to define what the dimensions of cyber risks are and what quantifies as an economic or humanitarian crisis. Economic impact, network effect, and severity are three distinct measures postulated as aspects of what makes a catastrophic cyber risk. The economic impact is the summation of business loss from network or data unavailability, spending for workforce surge required to understand, fix, and control the cyber problem, lingering business or reputation effects that result in lost sales, and cascading impacts due to supply-side and demand-side cascades of effects from the perturbation. Network effects are the result of the heavy reuse of software libraries, standardized operating systems, and similarity of configuration, combined with high levels of connectivity across businesses and industries. The network effect is the result of systemic rolling outages caused by these layers of cyber interdependence and makes the forecasting of economic impacts more nonlinear and less predictable than non-cyber hazards or perils. Severity is the degree to which an incident is unpleasant or serious. Such severity is seen in how an incident impacts a particular entity or series of entities. Likewise, physical manifestation, irreversibility, and systemic nature (e.g., Not Petya[2]) would be dimensions of catastrophic cyber risk.

The impact of a cyber incident is a significant factor to consider in categorizing it as a catastrophic risk event. Panelists note that security requirements like the FIPS 200[3] mention the scope of the impact and the nature of the impact, which may help define catastrophic cyber risk as it allows entities to measure the level of impact of an event directly. For example, we can look at how catastrophic risks are calculated regarding loss of life and economic impact outside the cyber realm. Critical impacts can include events that affect the health and safety of individuals and disrupt an organization's ability to accomplish its mission. Here the rippling effects of an attack may accentuate the catastrophic cyber risk. Participants agree that the impact on quality of life is an essential dimension, where the inability to carry out daily tasks (e.g., disruption to fuel access) may be catastrophic. At the national level, the health, safety, and security of the state are critical.

Catastrophic cyber risks can also be defined via a significant amount of harm impacting assets, individuals, or operations of insurance companies or insureds. Yet, even within this, how one defines a significant amount of harm may vary greatly. Catastrophic cyber risk is seen as an instance where both financial losses and physical damages are

[2] Not Petya was a ransomware attack targeting Ukraine but with global impact. See the following link for more information: https://www.cfr.org/cyber-operations/notpetya

[3] FIPS 200 is a standard for federal agencies on the minimum security requirements for federal information and information systems. More information can be found here: https://csrc.nist.gov/publications/detail/fips/200/final

high. At this avenue, if a critical infrastructure is brought down, it would be deemed a catastrophic event from an operational and societal perspective.

Other experts in the panel share that it is important to consider what it means to be a catastrophic cyber risk. In this, how closely does a catastrophic cyber risk have to be tied to a cyber incident? In this case, does a cyber incident lead to a physical issue that leads to another issue? When would such a thing stop being a cyber risk? Is a cyber risk not being able to fill up at a gas station, or is that too far removed from the incident itself? Here we must ask the question of what is insurable versus what is not when evaluating the definition of catastrophic cyber risk.

The aftermath of an incident can also make it catastrophic, as noted in the discussion, where price gouging and increased prices for necessities like water, gas, etc., can result in a catastrophic risk to life and order. In this, there were justifiable concerns that such a catastrophic risk could cause cybersecurity insurance premiums to increase and result in irreversible damage for said insurers. The scarcity of incident response resources, whether supplied by insurance carriers or not, was also considered part of a widespread catastrophic cyber event.

Catastrophic cyber risk is also defined by the target of an attack. In today's connected world, panelists agree that the effects of a cyber incident can propagate across society, whereupon, if it affects one company or area, it most likely will affect others. As such, catastrophic cyber risks can be seen if the main target of an attack is not a single organization but instead an attack that propagates through a network and impacts other companies. In this, a ransomware attack like NotPetya, a widespread worm, or a self-propagating attack is more likely to be catastrophic, as opposed to targeted ransomware which may impact a single entity. Some panelists cite the Log4J[4] vulnerability, where many players are affected in their ability to conduct operations, while other participants disagreed, stating that Log4J vulnerabilities cause almost no loss from an insurance perspective.

Along the same line, some define catastrophic cyber risk based on the view of specific players. An individual company may view going bankrupt as a catastrophe, whereas if multiple organizations are affected to this level, larger organizations, such as the government, might view such an event as catastrophic, as discussed above.

Panelists frequently referred to examples to help understand how catastrophic cyber risks should be defined. In the case of SolarWinds[5] or Colonial Pipeline[6], the reputational damage faced by the United States and its impact across multiple sectors make it a catastrophic cyber risk. It was stipulated by several panelists that the knock-off effects of the Colonial Pipeline attack can be seen as a catastrophe, as it impacted the supply chain and gas stations across the East Coast. Yet, other panelists cited that in cases like SolarWinds, although the impact did not reach a catastrophic level due to the mitigation efforts, the access the vulnerability provided to the attackers across the industry could have led to a catastrophic incident. Other examples, such as the Target breach[7] and Equifax,[8] were discussed in the context of catastrophic cyber risks, as they both impacted millions but damages and physical harm was low. In the

[4] The Log4J vulnerability stems from an exploitation of critical remote code execution (RCE) which opens countless consumer and enterprise services, websites, and applications to increased cyber threats. More on this vulnerability can be found here: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

[5] The 2020 SolarWinds computer hack was one of the largest and most sophisticated cyber operations on the digital supply chain to date, impacting federal agencies and operations, private sector companies, and state and local governments across the country. More on the SolarWinds attack can be found in the following policy paper: https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack

[6] The 2021 ransomware attack on Colonial Pipeline is one of the significant attacks on CI in the nation's history. It caused the company to halt all pipeline operations to contain the attack, causing a shortage of nearly half the East Coast's fuel supplies, increased prices at the pump, and public panic given the unknowns at gas stations. More information about the attack and impact can be found here: https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

[7] In 2013, Target faced a major data breach which led to several point-of-sale systems being compromised leading to millions of customers personal and financial data being leaked.

[8] The 2017 Equifax data breach was one of the largest cybercrimes related to identity theft, with over 150 million records of people across the US, Europe, and Canada compromised. More information about the breach and impact can be found here: https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc

case of Target, it was stipulated to reach catastrophic levels; a breach would have to impact several companies, like Target, Walmart, and Kmart, essentially reducing shoppers' confidence in using credit cards and shopping at box stores.

In some cases, panelists discussed whether catastrophic implies something irreversible. For example, in scenario planning, take for instance: a company that is selling products that improve the connectivity of a hydroelectric station, with one of the customers managing a dam that was upstream from a capital city, and an attacker hacks into the gate controls, opening them releasing water and causing massive flooding at the downstream city. A scenario like this is caused by a single-point attack but would cause a systemic incident with permanence. It would take a long time for the city to recover. This would be a significant reputation loss for the company that is selling the products, leading them to potentially abandon the sale of the complete product line. Several other scenarios could be discussed here, say an attack on a wind farm that decreases their efficiency, making them seem unprofitable, causing the whole renewable energy market to crash, and leading those that invested in the technology to face high impacts and costs. These cyber events cause a tactile loss event which has the potential to trigger other insurance coverages, including property, flood, business, interruption, etc. But the question remains whether such an incident would be considered catastrophic for the insurance industry.

1.2 CATASTROPHIC CYBER RISK FOR THE INSURANCE INDUSTRY

To begin, many definitions of catastrophic risk from the insurance industry started by laying out catastrophic risks in the physical world. In the insurance industry, from an actuarial perspective or what the Insurance Information Institute (III) uses to track catastrophic risks, an incident such as flood, hurricane, earthquake, or terrorism event where there's an associated dollar value, and there is a number of both policyholders and insurance companies affected with a total cost that exceeds a certain threshold is considered a catastrophe. Many of the panelists seek to define catastrophic cyber risks based on existing definitions of catastrophic exposures in the physical world.

There is a difference between how insurance companies view catastrophic cyber risk versus how the government looks at catastrophic cyber risk. As it stands, there is not a single, widely accepted standard definition for catastrophic cyber risk. Even if there was one, it would depend on what lens one would want to view it through. Even in the insurance industry, viewing catastrophic cyber risk through a financial lens is vital. There is an effort to define catastrophic cyber risks in regards to their nature, based on an attack on a specific firm or attacks on multiple firms at scale at the same time.

The current cyber landscape looks much like the counterterrorism landscape did pre-9/11. The impacts of 9/11 were felt around the world, with multiple lines of insurance impacted (i.e., property, life, marine, etc.). While several recent cyber attacks, including SolarWinds and Colonial Pipeline, changed the way several entities view cybersecurity, "silent cyber[9]" signifies the potential losses stemming from traditional policies that are not designed to cover cyber risks. A single point of failure that impacts many leading to many claims would be catastrophic for the insurance industry. For insurers, a catastrophic cyber risk is where a large number of policyholders are impacted. Therefore, a systemic vulnerability that leads to a widespread incident that can be claimed is a catastrophic risk. Systemic cyber exposure was discussed as referring to an exposure that has the potential to affect many clients due to commonalities or shared elements of exposure, while catastrophic refers to a systemic risk that manifests into severe or significant losses for many policyholders.

[9] Silent cyber refers to the potential cyber exposures that may be present in traditional property and casualty (P&C) insurance policies, where such cyber risks may not be implicitly included or excluded. Traditional P&C policies do not specifically refer to cyber and as such could be required to pay for claims for cyber losses in particular circumstances (e.g., a fire caused by a cyber attack on a printer).

For a cyber incident to truly impact the insurance industry, it must have a significant impact. From an insurance industry's perspective, a catastrophic event is an event that hits a high number of insured at the same time to the point where the insurance company's ability to pay claims is taxed. Similarly, the insurance industry defines a catastrophic cyber risk as an instance where an insurer faces multiple claims simultaneously from multiple companies. If this occurs, they will use support from reinsurance companies that are sharing the risk in different ways. In the case of an act of terrorism, entities may refer to the Terrorism Risk Insurance Program[10] if it goes past the financial ability of both the insurance companies and the reinsurance companies.

According to the discussion, the definition of catastrophic risk should be tied to money loss and incidents that are correlated across many events that trigger enough aggregate claims to exceed the cost. The insurance industry is always concerned with a cyber event that affects networks and non-tangible data that then translates into a kinetic loss of physical property loss or bodily injury loss. Such an event may trigger not just a cyber insurance policy but would affect property insurance and crossing policies. This is what an aggregate event will look like. The war exclusion is in policy language, although its applicability is contentious. This often brings an aggregation issue due to the scale of the incident.

There is a lack of consistency in cyber insurance coverage, particularly in the proprietary coverage forms. Many insurers have added clarifying language to other forms of insurance policies to not pick up silent cyber, but in some instances, cyber risks may be covered through part of other policies. Panelists discussed how insurance policies respond to both proximate loss and the resultant loss. For instance, the proximate loss could be a cyber incident that releases water from a dam, and the resultant loss is the water and the damage it causes. Insurers draw this distinction.

An additional concern faced by the insurance sector is many claims being placed at once can lead to insolvency. Currently, a majority of the claims that the cyber insurance industry is dealing with are ransomware incidents. Yet, cloud failure is one of the biggest fear of insurers and companies as it could cause mass-scale business interruption. For instance, the failure of a major cloud provider (e.g., AWS, Microsoft Azure, or Google Cloud Platform) may take down half its business portfolio, and many claims may have to be paid simultaneously.

While examining catastrophic cyber risk in the insurance industry, what is covered by the policy as a result of a cyber event needs to be considered. The common coverage areas of cyber policies include IT forensics, breach notification, public relations, and third-party liability, which are the insurable costs. In the case of reputational harm to a product manufacturer, some cyber policies build in reputational harm, although they are almost always sublimated. Insurers quite rationally have scoped down the elements that will be covered, where to fit a catastrophic event, the incident has to fit into one of the buckets, or the consequences could spill over in non-cyber claims.

In particular, insurers have various definitions of how they view catastrophic cyber risk. Some panelists state that catastrophic cyber risk could be defined as a widespread event that affects around 10+ insurance companies and 100,000 policyholders and has over $100 million in losses. Other participants define catastrophic cyber risk from the perspective of cyber as a risk profile that would be considered catastrophic. In this, a single insured could have a $100 million loss, but it is not labeled as a catastrophe by the insurance industry. Still, other participants disagree, stating that if 100 insureds have an aggregate loss of $30 million, that may be labeled a catastrophe by the insurance industry. The Property Claim Services (PCS) have a specific definition of a catastrophe. This definition is a

[10] The Terrorism Risk Insurance Act (TRIA) is a federal program that provides a system for public and private compensation for certain insured losses resulting from certified acts of terror. https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/federal-insurance-office/terrorism-risk-insurance-program

$25 million loss over multiple companies and several people. Panelists shared that $25 million may be too low in defining a cyber catastrophe.

Other participants dispute the above claims and state there was nothing that the insurance industry had not seen before. The implications for cyber insurers are minor compared to the other kinds of insurable events that have happened in the past. One participant shared that although there is potential for extreme cyber impacts to the cyber insurance sector when we look at the historical massive-scale cyber failures or even estimate what it could look like, the impact would still be small compared to incidents in other sectors. In this, from a cybersecurity standpoint, the financial impacts are minimal as such catastrophic incidents have been seen all before in terms of. If the insured losses and expenses arising from a particular event exceed the collected premiums and investment income though, it would be catastrophic. This would trigger further hardening of the market, increase underwriting scrutiny, and pull back terms and conditions toward future uninsured losses. Yet, still, others dispute those unforeseen events or the incident that falls through all the cracks of the insurance strategy. Such incidents are those that insurers have not begun to project yet, such as Stuxnet[11], Titan[12], and SolarWinds, which are all first-time scenarios.

There is an infinite number of cyber catastrophe scenarios, and it is not possible to enumerate all of them. One panelist shared that all cyber models are wrong, but some are better and more useful. Despite this, cyber insurance relies on modeling, where current models seek to shed light on what the mass cyber incident may look like (e.g., mass ransomware or a cloud failure). Many models exist on cyber-physical scenarios, including a dam failure; while cyber risks to said systems are not necessarily insured, they have the potential to be a catastrophe for the insurance industry.

Although modeling has improved over the years, panelists agree that many challenges exist. One challenge is historical cyber data, and changes to attacks make cyber risk modeling and projections tough. Additionally, panelists share that the plethora of data breach cost calculation benchmarks from a first-party loss perspective and the rising costs of litigation need to be reviewed. Accumulation risk is a major problem for cyber.

Likewise, using insurance as a metric to judge the criticality of an event may not represent the said event due to costs not represented, such as underwriting, reputation loss, and intellectual property theft. For small businesses, insurance penetration is lower. This would create an underrepresentation of the actual loss of an incident. For instance, the WannaCry[13] incident supports this, and insurers would not deem this as a catastrophic incident.

The National Institute of Standards and Technology (NIST) and the Federal Information Processing Standards (FIPS) guidance have been essential resources for insurers as they conduct risk assessments of IT systems in the government. The Department of the Treasury has put out a request for information (RFI)[14] to the public, including the insurance industry, but there has been some hesitancy in participating. The government plays a key role in setting standardization across industries. Yet, participants share that there are few government standards for the cyber insurance industry to date.

[11] Stuxnet is a malicious computer worm that was discovered in 2010 and targets supervisory control and data acquisition (SCADA) systems and is responsible for substantial damage to Iran's nuclear program. More information can be found here: https://www.cisa.gov/uscert/ics/advisories/ICSA-10-238-01B

[12] Titan Rian was a string of cyber operations targeting and breaching several US and UK government agencies. More information can be found here: https://www.cfr.org/cyber-operations/titan-rain

[13] The 2017 WannaCry ransomware attack targeted computers running Microsoft Windows, encrypting data and demanding ransom for computers around the globe. More information can be found here: https://www.cisa.gov/uscert/ncas/alerts/TA17-132A

[14] The RFI from the Department of treasury is available at https://www.federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-to-catastrophic-cyber-incidents and the public comments to this RFI are available at https://www.regulations.gov/docket/TREAS-DO-2022-0019/comments

In the insurance industry, panelists discussed how things transfer between property damage and cyber claims. Participants shared that a worst-case scenario for the insurance industry would be a cyber-attack on one system that causes widespread fires. Fires are a fundamental part of a P&C policy, so they have to be included, regardless of the cause. In such an instance, there is a need to investigate limits as mass damage due to fire caused by cyber would be a disaster and catastrophe for insurers.

In many instances, questions were raised regarding whether definitions exist to help in scenario planning and modeling. To better define catastrophic cyber risk for insurers, we need to understand the low limits for many cyber policies and risk-sharing capabilities of insurance.

In the insurance industry, after a large-scale attack, insurance carriers have had to answer questions for every vendor's claims for months to years as they viewed it as a systemic risk to their cyber risk book. The main reason behind this is that the exposed vulnerability unpatched would let the bad actors continue to wreak havoc on the systems (e.g., ransomware payloads). Attacks like NotPetya, on the other hand, would be considered a single attack, not one that arrives at catastrophic levels.

Many cases of cyber incidents are being discussed in the insurance realm. Instances include Mondelez *v.* Zurich case and NotPetya cyberattacks, although the coverage was through an all-risk property insurance policy. Another example could be an attack on the electric grid. This attack would have cascading effects across multiple industries and areas. We obtain real-world examples of this through Russian attacks on Ukrainian power grids. Regarding the physical realm, Hurricane Sandy and other catastrophic events have shown how other critical services, such as the food supply chain and gasoline, fall apart.

1.3 ISSUES WITH DEFINING CATASTROPHIC CYBER RISK

Given the expansive nature of which panelists defined catastrophic cyber risk, along with the diversity in their expertise and experiences, it is not surprising that a variety of issues were brought up regarding the current state of catastrophic risk. Issues that were mentioned when defining catastrophic cyber risk include:

- Insurers and insureds define catastrophic cyber risk differently – In this, insurance buyers typically define catastrophic cyber risk as one that has an economic impact, network effect, and damages to their business mission, individuals, or financial outlooks. For many entities, a catastrophic cyber risk may impact their business model or harms individuals. In this, the Target breach may be considered a catastrophic cyber incident by Target Corporation, but by insurers, not so much. Insurers view catastrophic cyber risk as a systemic vulnerability that leads to widespread incidents and claims.

- Unclear dimensions of catastrophic cyber risks – A common language of how we measure catastrophic risks is lacking. Economic impact, network effect, and damages are the three distinct measures of catastrophic risks we need to get to a clearer definition of. How do we measure the impact and severity that create a catastrophe?

- Known unknown cyber risks – Although cyber risks may be generally understood, the scope and nature of the impact, the sophistication of the attacks, and the frequency typically are difficult to estimate accurately. In this, arriving at a standard definition of catastrophic cyber risk for all entities may be very tough, as the risks and potential impact may waver dramatically from industry to industry.

- Threat of physical harm – There may be a delineation based on a public standpoint that catastrophic cyber risk is considered to have some cyber-physical harm associated with it. The losses are not very clear when there is no physical harm. So, unlike catastrophic risks caused by floods or hurricanes, defining catastrophic cyber risk based on physical harm or loss of life may be a challenge.

- **Damage estimates –** There are many court battles down in Florida as people recover from the recent hurricanes and debate what damage was caused by wind, which is conceivably covered, and flood, which is probably excluded. Most property insurance policies have written exclusions that do not cover what would traditionally be covered on a cyber insurance policy. So, property insurance policies indicate that if there is an incident, the insurer will not cover IT forensics, breach coaching, notification costs, and class action lawsuits' defense; instead, the insurer may only cover the physical loss on the property policy. And even then, the loss has to arise out of a covered cause, i.e., something that is not already excluded.

- **Quantifying cyber risks is tough –** In this, is an impact on 10,000 businesses catastrophic, or does it have to be an impact on 100,000 businesses? How the buyers of insurance and insurers quantify cyber risks differ, as the frequency and severity of an attack may constantly change.

Many panelists shared that viewing catastrophic risk from the insurer's perspective is much different than those seeking insurance, as the human/personal element is not considered, as cyber risks are only insured for businesses or entities. Within this, several issues are raised in defining catastrophic cyber risk, given the current state of cyber risks.

Section 2: Managing Catastrophic Cyber Risks

Next, the panelists reconvened into three groups in breakout rooms and asked to discuss: How does the insurance sector handle catastrophic cyber risks (tools, techniques, and data)? A summary of the discussion that ensued is given below.

2.1 TOOLS, TECHNIQUES, & DATA TO HANDLE CATASTROPHIC CYBER RISKS

There are several ways in which catastrophic cyber risks are handled. There are a lot of methods used in the pre-policy/underwriting process, including InsurTech solutions, proprietary scanning and risk evaluation tools that inform the underwriting process, and application questionnaires.

2.1.1 INSURTECH SOLUTIONS

The marketplace is starting to see the explosion of InsurTech solutions. While some carriers previously may have stayed away from some of these InsurTech solutions, they had exponential growth. Some of the tools were especially deemed useful for the middle market since some of the large clients can be more sophisticated and do not need the InsurTech tools. So, the InsurTech solutions are providing not only pre-agreed services, but they are also providing constant alerts where they can identify whether their policyholders are getting hit or there are new variants of attacks coming out. The InsurTech solutions push out notifications or patches, and sometimes, can be seen as similar to a protective Big Brother.

2.1.2 THIRD-PARTY SCORING

Another available method is third-party risk scoring reports (e.g., by BitSight, Security Scorecard, and Cyber Cube) that help mitigates catastrophic cyber risk. While some panelists used third-party scoring tools like BitSight and Security Scorecard to conduct vendor evaluations, many stated that depending on the tool and input data were not overly reliable. Also, these risk scoring products can provide a better view of risk for information-technology-focused industries than for operational-technology-focused industries. These massive, easy-to-collect data misrepresented the organizations' ability to develop secure products and maintain secure operations. Essentially, all the methods try to provide better measurement of the security levels of insureds and hopefully raise that level.

The goalpost continues to move as insurers are requiring and increasing the bar from a technical control perspective. If the clients do not follow the technical control requirements, the insurers may not provide coverage.

2.1.3 RISK MODELING

At the forefront of addressing catastrophic cyber risks is modeling. As participants share, insurers often use models as tools, not as answers. Insurance modeling is not trying to predict the future but seeking to predict next year via near-term prediction and estimating (as most policies only last 365 days). Panelists agree that modeling cyber risks present a conundrum.

Modeling takes lots of guessing and reliance on expert judgment. Lots of data, including frequency, severity, and financial loss data, are needed to create a reliable model. Once insurers have the results of the models, it helps brokers determine limits and whether premiums are right and place insurance portfolios with reinsurers looking at aggregate risk (e.g., if Amazon Web Services (AWS) are down for a week, how much will it cost the whole portfolio?).

Modeling cyber risks is tough as cyber risk and exposure are constantly changing. Here the types of attacks and targets are changing, and technology is continually developing. Where there is a hard target, many attackers will move to an easier-to-exploit entity and lower-hanging fruit. With technology changes, the targets keep moving and shifting.

Measuring frequency is another challenge due to the unknown and constantly changing nature of cybersecurity. Some people may get confused about statistics and modeling presented on the news or social media. In this, 1 in 100 is the same as 1%, so it does not mean the event is only supposed to occur every 100 years but has a 1% chance of occurring. On the other hand, FLAKE modeling is conducted using the likelihood of an event occurring within a given time period.

Earlier cyber models were not the best predictors of future incidences. Although many scenarios are modeled and plausible, extremely rare risks are seldom modeled as knowing frequency is a challenge. For example, there are currently no quantifiable models for cyber-attack that causes fires (i.e., a hack on a printer vulnerability causing it to overheat and start mass fires). Likewise, the increased rate of frequency of attacks in small to medium-sized enterprises (SMEs) is bending the modeling curve.

The industry has been trying to build some models internally to project the revenue at risk stemming from a lack of a secure development lifecycle. Additionally, they lose market share, resulting in sustained revenue loss across the product's lifetime. So, they have to balance: do they spend more time finding all the weaknesses and vulnerabilities before they push a product out? Or do they lose market share and have sustained revenue loss? After such modeling, it is determined that one may not know anything and is trying to project things off of bad data. In accounting for the uncertainties in data, the resulting projections do not help insurers or buyers of insurance make decisions.

More specifically, catastrophic (CAT) modeling looks at what the catastrophes could look like and what the loss distributions might look like in the future. CAT modeling is done to analyze the scenarios and aggregate risk so they can come up with models and loss distributions that could see what happens if one of these catastrophes happened so that they could then price their insurance accordingly.

2.1.4 UNDERWRITING APPLICATIONS

Also, there are applications a client needs to respond to from an underwriting perspective to buy cyber insurance coverage. These applications ask about the current technical standing and cyber risk practices, like what did the entity do about Apache Log4j, was the entity a subject to SolarWinds, etc. So, there are more attempts to ensure that baselines are being met to head off some of the catastrophic risks preemptively. One panelist shared that although the questions insurers ask are reactionary and related to significant historical events, they still provide insights into how competent the insured's security posture is.

Applications across the industry are costly because they require a lot of time and effort to gather the data and be as a representative as an insurer or client wants them. But they are so easy to defeat. A lot of these applications try to ask yes or no questions or categorize all answers. However, sometimes the answers do not fit into any of the categories. So, buyers of insurance end up just picking up the one that makes them look better. Buyers of insurance may not pick the one that makes them look worse because there is ambiguity about which categories fit into other categories. If there's a statement like that, in some of these applications, the entity cannot get the right answer because neither answer is correct. There was recently litigation in a Midwestern state where carriers began denying claims because insureds did not do exactly what has just been described. To address this, the carriers counsel clients to add an addendum if an answer is a maybe or it depends.

However, processing this data might be challenging. Therefore, replacing the application method with a more effective one could be a good strategy for the insurance industry. For example, Equifax now publishes for their customers an online dashboard that gives real-time data across hundreds of controls. It tells its customers a significant amount of detail about what is going on today. Then, what one sees when vulnerabilities emerge, customers can see them show up on the Equifax dashboard, and they see what their capabilities are to fix those things.

According to one participant, per their experience, 60% to 70% of cyber claims occur at $150 million and lower revenue companies that were already struggling with their IT budgets. They do not have a Chief Information Security Officer (CISO), and they barely have an IT director. How is that insured going to help manage that process? These companies also do not have sound compliance and audit practices, which also makes their responses to the questionnaires even less reliable.

Cyber insurance applications have evolved: they used to be very long, then got short, and now going longer again. Insurers may want to have an in-person meeting with the system architect and system engineer. Rather than having an application, they want to have a conversation with key personnel. So, a respective buyer of insurance can demonstrate or speak to the safeguards in place and the things currently done to protect the entity.

2.1.5 CYBER DATA

Insurance carriers are being pushed by reinsurers, rating agencies (e.g., S&P and AM Best), and other interested parties to get a handle on what their aggregation risk looks like, with insurers at varying maturity in this. There are data sources to determine aggregate risk or maturity, but none are particularly good. There is a move to address this with data, but cyber insurance has just past its infancy and is not mature yet.

Yet, even then, issues remain in seeking cyber data. Panelists agree that cyber data is not of the highest quality. While data has penetrated the underwriting world, it is also penetrating the aggregate cyber risk domain as well. However, compared to other catastrophic event data (e.g., hurricane data, flood data), catastrophic cyber data is limited due to the lack of historical cyber data.

There are multiple sources and types of data that are used. One panelist said that they use 3 different modeling tools, average them, and add 20% for their reserve guidelines. This speaks to the lack and unreliability of data. There is also a lot of synthetic data that is built out using simulations such as Monte Carlo. Further, there is publicly available cyber data, including public data around losses, but there is very little publicly available data about the attack vector. There is very skewed data on this due to the vendors that are publishing these reports.

2.2 EVALUATING CYBER RISKS

Exclusions in policy coverage and underwriting have allowed insurance providers to avoid having events deemed catastrophic in the eyes of the insurance industry. Lloyd's recent guidance states that any syndicates that are writing policies for cyber should improve language and include war exclusion verbiage. This may allow the insurance industry to eliminate some catastrophes with a pen, even though this is still debatable. For example, all cargo insurance policies use the same language regarding cyber exclusions, as recommended by Lloyds. However, there is the ever-looming threat of the unknown risk being exploited and legal challenges.

Panelists shared what is being done in the insurance sector, both in insurance brokerage and reinsurance brokerage. In this, there is a standard process used to evaluate cyber risks to an entity:

1. Firmographics (i.e., companies, revenues, industries, geographic locations, etc.). Reinsurers supplement firmographics with benchmarks from industry

2. Historical incident claims data (severities, impact, geography)

3. Technographics include outside-in and inside-out data. Inside-out data includes a cyber risk assessment (i.e., approx. 150 questions) to get the cyber insurance spectrum from very confident to not confident. Inside-out data is indicative of claims.

4. Cyber modeling (e.g., cyber cube models, RMS).

Yet, standard processes and models present skepticism among insurers and insureds. Questions arise, including if cloud providers should accept some risk. Should insurance providers ask cloud providers to cover some of the loss? Here there is some level of service level agreement, but it does not cover the systemic level of risk. Along with this discussion, some participants think organizations do not have any leverage to negotiate a contract with cloud providers. It is mentioned that the locus of power is around the cloud provider, and they do not want to accept this level of risk.

The discussion then moved to CAT bonds in cyber. In the insurance industry, CAT bonds are common. But, in the cyber realm, cyber models are relatively new, causing a reluctance to invest in cyber CAT bonds. Given there are no geographic or industry limitations with cyber, CAT bonds for cyber are still in the early stages. Yet, panelists agree that CAT bonds will be seen in the future.

Section 3: The Changing Cyber Risk Landscape

Next, the participants were asked to discuss the question: As the cyber risk landscape changes, has the insurance industry been sufficiently proactive (or reactive) in responding; for example, how well did the industry respond to the 2016-2021 evolution of the ransomware problem? The discussion that ensued is as follows.

3.1 THE INSURANCE MARKETPLACE

The discussion moved toward the changing cyber risk landscape and whether the insurance industry has been reactive or proactive in responding to risks. Many of the panelists stated that this is the wrong question since the insurers have to be reactive as there is no way to be proactive in the current cyber landscape. In this, it is hard to be proactive in cyber, as it is not something that can be predicted.

Yet, others think that insurance providers have been proactive. Coverage started back in the early 2000s and only has hardened over the past couple of years. The market is starting to contract with tougher underwriting, more exclusions, etc. However, the current offerings are broad. In modeling and scenario analyses, one can determine the cyber risks presented and how said risks may fit certain insurance policies. Some of the participants share that cyber claims are down. This is attributed to the fact that underwriting is getting better, despite increased risks. In this, insurers have become more proactive in the loss control space, providing tools to increase the security postures of the insured.

What drives coverage is what is profitable for the industry. Industry’s reaction to the risks to the small, middle, and large-sized markets vary greatly. Various carriers, appetites, and requirements within these sector segments can be different as they may gravitate towards a single large loss from a large company or multiple insured events from smaller companies.

The cyber insurance market is changing due to the current landscape. Yet, the penetration of cyber insurance is still low. In this, the increased risks and various levels of cyber hygiene have forced insurers to up their requirements and create more detailed cyber risk assessments. Attackers will keep moving to low-hanging fruits as others have stronger IT systems and protection.

One value of a cyber insurance policy is the services that are offered with the policy. By purchasing policies, smaller companies get resources such as computer forensics on retainer, a breach coach, and legal assistance to navigate the complex regulatory landscape. The value does not just land in the financial transfer but in response to an incident. Likewise, insurers can help with discounted risk assessments, security awareness training, and more.

The discussion also shed light on small businesses and how they may not have the resources to respond. Questions were raised on this topic: How does the insurance industry help small businesses not cause catastrophic cyber incidents? How can the insurance industry get clients more concerned about cyber?

Most of the improvements that can be made to address cyber risks may reduce the risks that entities face by a large percentage. Yet in this, many may not have an IT department due to budget restrictions or outdated software (i.e., this is an issue for the government and small businesses). Oftentimes, critical infrastructure (e.g., hospitals and electrical grids) have outdated and vulnerable systems and software, which require upgrades. The public sector and municipal government challenge parallel small businesses, where limited resources and expertise limit the ability to proactively prepare for an incident. Yet, some note that many entities will just have to deal with outdated systems as updates are not cost-effective or currently an option.

3.2 EVOLUTION OF RANSOMWARE

The discussion then sought to better understand how the industry responded to the evolution of ransomware between 2016 and 2021. Unanimously, ransomware is noted as the main driver of the recent cyber insurance evolution and rate increases. The requirements over the past 4-5 years have changed the insurance marketplace, where insurers have tried to address rising ransomware attacks with increased measures. Some ways in which the industry has changed due to the evolution of ransomware include:

- Insurers are seeing more cyber claims than ever.
- Many insurers are conducting longer cyber risk assessments to determine insurance eligibility.
- The focus of cyber insurance underwriting has moved from evaluating third-party liability to evaluating incurred first-party breach response expenses.
- Insurers have responded by changing underwriting guidelines by requiring security hygiene and more cyber risk management technical controls, including:
    - Multi-factor authentication (MFA)[15]
    - Offline backups
    - Privileged administrator access
    - Elevated privileges[16]
- The emergence of the Business E-Mail Compromise (BEC) has resulted in further discussions on ransomware. Likewise, social engineering coverage started after BEC, as "willingly" giving money away is not a covered claim.

[15] Multifactor authentication is a layered approach to securing data and applications requiring a user to present more than two credentials to verify their login. https://www.cisa.gov/publication/multi-factor-authentication-mfa

[16] Elevated privileges are when a user is granted the ability to do more than a standard user.

Section 4: Catastrophic Cyber Risk Scenarios

Next, the participants were asked to discuss the sectors and types of scenarios that would benefit cyber risk management and the cyber catastrophic risk realm. The discussion resulted as follows.

Reliance on scenario analysis and modeling is central to understanding cyber risk both for insurers and buyers of insurance. Experts shared that depending on how cyber catastrophe is defined, the sectors that a scenario may change. One sector scenario may lead to more financial losses, but another might have health or safety impacts and potentially lead to loss of life. Technology monocultures can enable attacks on one system that exists across a sector or geography and thus could take hundreds of hospitals or healthcare facilities offline or impact several electrical grids. Attacks on communications infrastructure, like undersea cables, could also have widespread impacts across sectors or locations.

There was an important discussion about whether scenarios should focus on improving currently discussed and modeled problems or attempt to address novel and underexamined ones. Some panelists felt that scenarios should focus on challenges that have yet to be investigated. In contrast, others suggested that more should be done in currently studied areas to fully understand systemic impacts. Based on the group deliberations, several sectors and areas that present catastrophic cyber risk scenarios emerged:

- *Sector-Specific* – healthcare and large hospital organizations, the financial sector, the insurance industry, etc.
- *Critical Infrastructure* – the power grid, telecommunications, water and wastewater, pipelines, etc.

In either a sector-focused or infrastructure-focused scenario, some themes emerged that seemed key to whether the scenario could or would reach catastrophic levels. The amount of centralization of the organizations and assets in a given sector and the shared reliance on infrastructure or software monocultures within or across sectors seemed to be potentially important risk drivers.

Several panelists suggested possible events or elements of a scenario that might be leveraged to create conceptually and practically useful red teaming scenarios for subsequent meetings. These include:

- Cyber attacks with physical consequences, not just on critical infrastructure systems, but for example, attacks on widely used hardware or consumer devices that could cause batteries to overheat and cause fires
- Attacks on pieces of infrastructure that are small in number and very high in consequence (e.g., attacks targeting undersea fiber cables or petroleum pipelines)
- Attacks on power systems that leave key devices, facilities, or sectors unable to operate, causing cascading impacts
- Attacks targeting widely used information technology services (e.g., cloud computing operators) or goods (e.g., software supply chain attacks)
- Attacks on sensitive healthcare goods or services that could undermine reliability or public trust (e.g., attacks aiming at pharmaceutical supply chains or the blood supply)
- Attacks on the insurance industry in which data is stolen and leveraged in subsequent attacks to understand what coverage clients have and what ransoms or payments might be extorted

- Attacks on public trust in elections were mentioned, not necessarily only on election infrastructure, but as part of a broader discussion around trust and reputational damage from the cyber attack, including the supposition that someone could conduct a cyber attack that leads to health impacts and deaths in one country, alter logs and conduct counter forensics, in an attempt to blame or attribute such an attack to another country

- Coordinated attacks (either multiple different cyber attacks, cyber attacks in conjunction with information operations, or the combination of cyber and physical attacks) were also a common theme in terms of what types of attack scenarios might rise to the level of catastrophe

Through all of these interesting and thought-provoking suggestions, what became clear is that concerns about data and device availability and data and device integrity seem at least as important about concern confidentiality when it comes to thinking about the potential for catastrophic cyber events. These themes provide important insight into what kinds of drivers and events might appear in subsequent scenarios for the red teaming portion of this project.

Section 5: Major Deficiencies in Handling Catastrophic Cyber Incidents

Following the discussion in Section 4, the panelists were asked to discuss the major deficiencies in analyzing and handling catastrophic cyber incidents. The discussion that ensued follows.

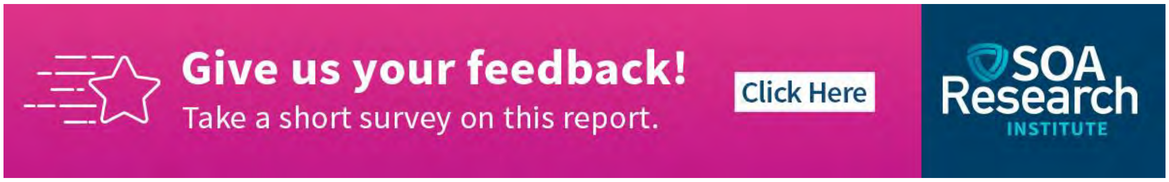
Several themes emerged in response to discussions about the deficiencies in preparing for and responding to catastrophic cyber incidents. The distinction between challenges to pre-incident and post-incident challenges was thoroughly discussed. Notably, the insurance industry (unlike some other stakeholders) has clear interests in improving both sides (as opposed to focusing on one or the other).

On the preparation side, there are numerous challenges in modeling and assessment processes for these events. These include:

- Sparse data, as in so many parts of cybersecurity, remain a major challenge. The challenges of collecting data, the incentives aligned against many organizations sharing data, and several other factors contribute to this.
- Modeling frequency is particularly important in the case of rare events, but especially in the case of events that have not happened yet.

On the response side, numerous challenges hinder smooth and effective recovery. These include:

- Organizational, cross-organizational, and communication hurdles is a key theme. In entire sectors, this is a challenge. Yet challenges exist at the level of victim organizations communicating with their vendors, clients, and partners, as well as their insurance carriers.
- Digital forensics and incident response remain expensive and time-consuming. Participants described cases in which numerous vendors and extensive auditing were required to ultimately complete digital investigations or remediations.
- The lack of scalable response expertise will be especially problematic if a catastrophic cyber incident occurs. Having enough claims adjustors, incident responders, and other kinds of technical expertise to respond to large-scale, geographically distributed, or widespread scenarios would result in a "demand surge" and costs. Examples of this outside of cybersecurity, like in response to hurricanes, were cited as illustrative examples.



Section 6: 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:

Seth Baum, Global Catastrophic Risk Institute

Nicole Becher, Google

Kenneth Crowther, Xylem

Gregory Falco, Johns Hopkins University

Ben Goodman, 4A Security and Compliance

Jim Haltom, DHS CISA

Howard Miller, LBW Insurance

Tyler Moore, University of Tulsa

Norman Niami, American Academy of Actuaries

Reid Putnam, Gregory & Appel Insurance

Marc Schein, Marsh McLennan

Scott Stransky, Marsh McLennan

Jeremy Straub, North Dakota State University

Daniel Woods, University of Edinburg

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, Assistant Professor

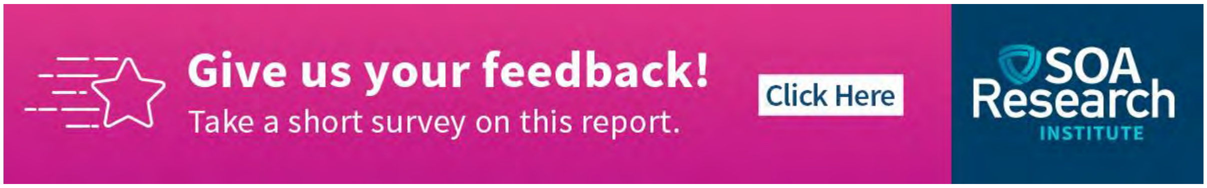
Brian Nussbaum, PhD, Associate Professor

Omer F. Keskin, PhD, Assistant Professor

Elisabeth Dubois, MBA, PMP

Dominick Foti, MBA

Feedback


Give us your feedback!
Take a short survey on this report.
Click Here
SOA Research INSTITUTE

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