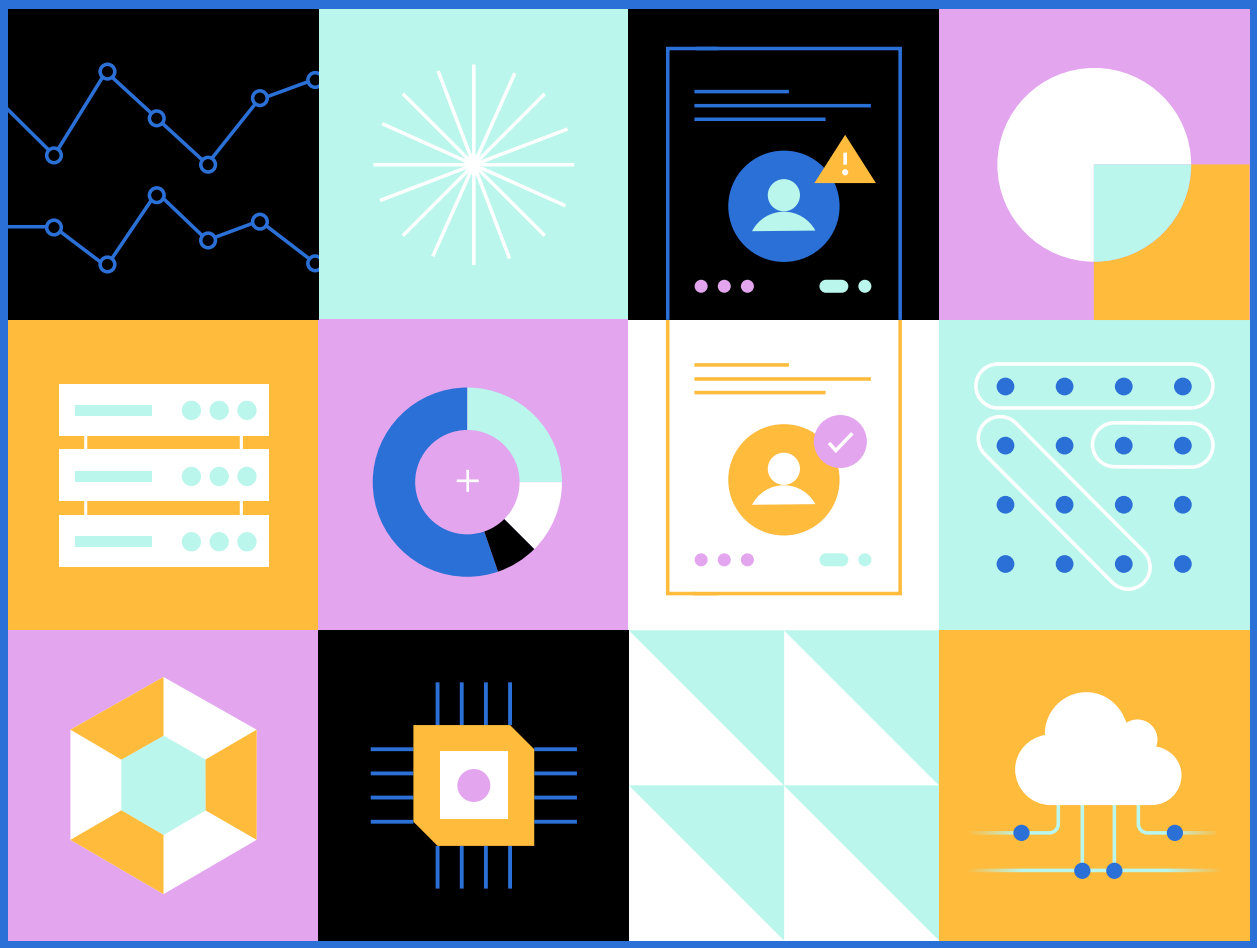
Coalition®

coalitioninc.com



Active Cyber Risk Modeling

A modern approach to cyber risk aggregation

Table of Contents

Executive Summary

Technology has become the bedrock of the modern economy, and most businesses rely on the same technologies to operate. This shared dependency on technology infrastructure creates aggregate cyber risk: a single cyber event can trigger multiple events that cause widespread catastrophic loss.

Concerns about catastrophic cyber risk have prompted questions about the long-term viability of cyber insurance. However, due to the vast amount of digital data available, cyber risk is one of the most knowable risks in the modern world. Cyber risk cannot be modeled like other risks and requires a new approach. To better understand and assess cyber risk aggregation, we developed Coalition's Active Cyber Risk Model.

Our model provides a framework for systematically monitoring and quantifying the financial impacts of a catastrophic cyber event. But rather than relying on the outdated methods and models of traditional insurance, we built our model from the ground up to leverage data from the businesses we help protect daily.

The key to cyber risk aggregation modeling is connecting cyber events to businesses and their technologies. By monitoring the shared technology among policyholders, we can remain current with the evolving cyber landscape and confidently see which technologies present the most significant cyber risks.

Coalition has exclusive access to extensive data, technically savvy teams fully dedicated to understanding cyber risks, and a vested interest in protecting policyholders. We share our approach because we believe a practical framework and understanding of aggregate cyber risk can unlock more sustainable underwriting models and stabilize the cyber insurance industry.

This report explores the critical distinctions between natural and cyber catastrophes, why cyber requires an entirely different approach, and how Active Insurance can mitigate cyber risk. We also provide an in-depth look at how we construct our model and explain why Coalition remains confident that cyber risk is insurable and that cyber insurance can play an essential role in the modern economy.

Introduction

In the same way property insurers worry that a hurricane could damage multiple properties, cyber insurers are interested in how a single event could cause digital losses across many policyholders due to shared technology infrastructure, such as cloud computing.

Historically, property insurers have addressed this concern by monitoring the location of insured properties and underwriting to avoid coverage accumulating in one local region. Many cyber insurers are working to understand what an equivalent strategy looks like in the digital world.

The uncertainty around cyber risk has led to conservative modeling. For example, market-leading cyber catastrophe models consider the possibility that all of Amazon Web Services (AWS) go down for an extended period, a doomsday scenario detached from the reality of geographically distributed data centers. The AWS cloud spans over 100 discrete data centers globally, each with redundant power, networking, and connectivity.

Born out of insufficient data, improper risk modeling, and a fundamental misunderstanding of how cyber risk works, this perspective sows narratives of fear, uncertainty, and doubt, ultimately resulting in the claim that cyber is “uninsurable.” Instead, cyber is likely one of the most knowable risks because of the wealth of data available in the digital world. Therein lies the challenge: capturing the correct data and implementing the right tools to manage the risk.

Why Cyber Requires a Different Approach

Because no precedent exists for a catastrophic cyber event, we rely on models and simulations, observe comparable areas of insurance, and leverage our cyber expertise to explore the possible effects. Past high-profile events, such as Kaseya and Log4J, are considered "near-misses" because they were widespread but didn't result in significant financial loss for the cyber insurance industry.

Decades of natural catastrophe risk modeling inform the industry-standard approach to cyber risk aggregation. However, cyber risk mitigation can occur proactively and in close to real-time, often at the individual loss level, leading us to conclude that cyber requires a different approach.

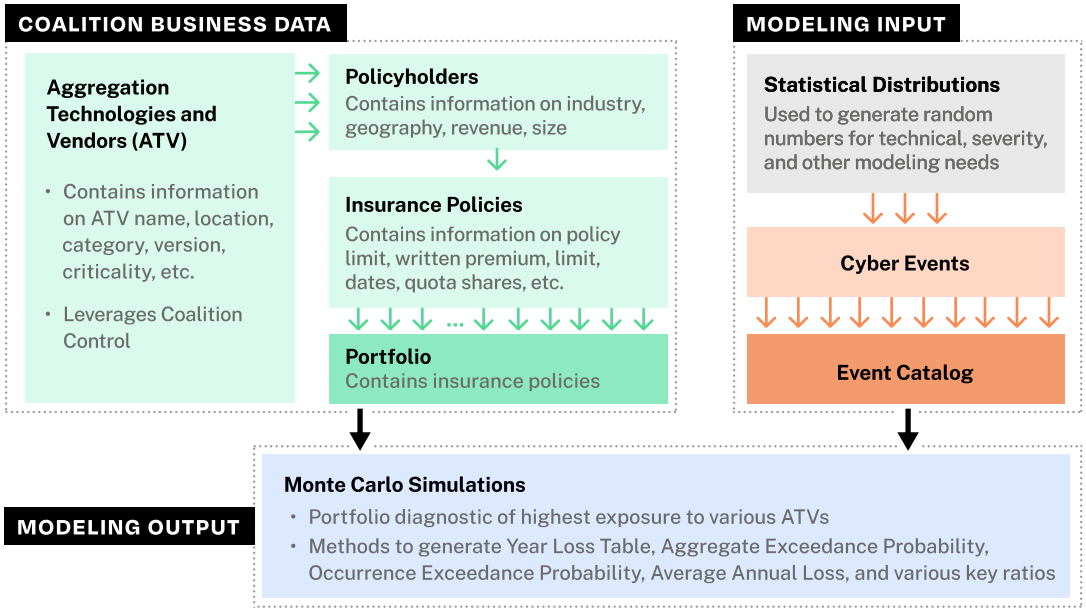
Natural catastrophe models rely on a combination of historical data and geographical maps. We know specific U.S. locations, such as coastal Florida, Louisiana, and Texas, have historical exposure to hurricanes. We can reliably assume this exposure will continue going forward, creating the possibility of systemic insured losses. Property insurers track their exposure to hurricanes through policyholder ZIP codes, used as input for natural catastrophe models.

To follow the natural catastrophe model, cyber catastrophe models face two problems. First, the historical record has little predictive value because threat actors innovate and shift to target novel technologies. Second, a cyber policyholder's ZIP code provides no information about their exposure to systemic cyber risk.

Coalition uses the digital equivalent of ZIP codes, namely Internet Protocol (IP) addresses, to model exposure and identify future sources of systemic cyber risk. Tracking and measuring our policyholders' externally facing internet-connected infrastructure helps us understand the technologies that could be impacted by so-called "digital hurricanes," which allows us to focus on realistic scenarios for cyber risk aggregation.

Our approach to cyber risk aggregation centers on our Active Risk Platform, a proprietary risk management platform that continuously scans the internet and collects data on billions of devices and tens of millions of organizations; our whole data set includes internet scans of 5.2 billion IP addresses. We also utilize an extensive global network of honeypots to learn the behaviors of potential attackers and gather intelligence on the vulnerabilities and software they are targeting.

Coalition's Active Cyber Risk Model



Aggregation technologies and vendors (ATVs), perhaps the most robust dataset that goes into our Active Cyber Risk Model, are the digital technologies and third-party vendors used by Coalition policyholders. These shared dependencies create aggregate cyber risk, and we use ATV data to track and measure the interconnectedness of technology and identify where cyber risk is aggregating in our portfolio.

Ground-up Modeling

The foundational element of our Active Cyber Risk Model is our proprietary digital data: a powerful combination of cybersecurity research data and policyholder data. We built our model from the ground up, which enables us to leverage data from the businesses we help protect. Coalition's laser focus on policyholder security gives us an edge in assessing individual cyber risks and understanding the cyber risk landscape.

Coalition's laser focus on policyholder security gives us an edge in assessing individual cyber risks and understanding the cyber risk landscape.

The universe of organizations we monitor, including our growing customer portfolio, provides us with invaluable risk insights. We actively monitor every Coalition policyholder and tens of millions of other organizations to identify their externally facing internet-connected assets and any associated ATVs. We also gather detailed information on both exposures and incidents, as well as claims data on policyholders and past applicants. We can connect cyber events to policyholders and their technologies using this data.

By design, our Active Cyber Risk Model can determine which ATVs present the most significant cyber risks — this is where traditional models in the market fall short. Legacy insurers and modeling firms often use non-proprietary data and third-party scanning technology to build their models. External data matching can lead to data quality issues and unreliable results. Similarly, outsourced scans often cannot gather the high-quality data necessary for credible risk modeling. Furthermore, these scans fail to collect data at a sufficient scale and speed to keep up with the constant changes to cloud infrastructure and a growing portfolio of policyholders.

Coalition doesn't have to make assumptions about policyholder technology because we built our data collection capabilities from scratch and collect all data in-house. Our model provides a framework for systematically monitoring and quantifying the financial impacts of a catastrophic cyber event. At the same time, the quality and granularity of our data enable us to remain current with an evolving landscape to state with certainty and in near real-time how and where we have aggregated cyber risk.

Simulation Engine

Our engine is how we set our data in motion to simulate catastrophic cyber events. The components of our engine are optimized to accommodate millions of trials and simulate a portfolio of individual policies. We can also adjust the various components of a simulation, including the event set, underlying statistical distributions, and portfolios.

Inspired by historical cyber events and future scenarios, we designed our simulation workflow to be systematic and representative of how an aggregation event might occur. The framework can be adapted to any industry or regulatory cyber event so that it is flexible to accommodate most types of cyber risk modeling needs.

Simulation Workflow

1. Start with the **Event Set** to determine the types of cyber risk events.
2. Select the **Frequency** component to get event realizations.
3. Select a **Root Cause** component to quantify the impact.
4. Select the target **ATV** (aggregation technologies and vendors) component for all event realizations.
5. Match simulated events with a portfolio to calculate financial losses based on the **Severity** component.
6. Use **Policyholder Details** to calculate insured losses.

Model Methodology

Created with modularity and flexibility in mind, our Active Cyber Risk Model is designed to handle various cyber events and includes those of particular interest to Coalition, as well as external industry-standard benchmarking cyber events. Below are all of the components required to parameterize different cyber events for the purpose of simulation.

Event Set

We use a set of eight different types of cyber risk events. Our event set is composed of outages impacting seven different categories of ATVs that result in contingent business interruption, as well as one event where a zero-day vulnerability is weaponized to carry out cybercrime, including ransomware. Curated by our security experts, the events in our event set represent realistic cyber risk scenarios.

Active Cyber Risk Model Event Set
Advertising outage
Content delivery network (CDN) outage
Domain name system (DNS) outage
Email outage
Hosting outage
Payments outage
SSL/TLS certificate provider outage
Weaponization of software susceptible to zero-day vulnerabilities

Outage event

Zero-day vulnerability

Events can be grouped in the model to enable simulations that realize multiple events over a period of up to one million years. Each event has its own set of parameters, such as ATV, root case, event frequency, and event severity. Additionally, our model picks ATVs that are more reasonable, such as a hosting outage in a specific cloud region on Google Cloud Platform or Amazon Web Services.

Frequency

Frequency determines the probability of event realizations in the model. For each event, we set frequency based on the probability of a rare event, such as a prominent vendor going down longer than the typical waiting periods in our policies. More than one event can occur during any trial year, though event realizations in our model are independent of one another, enabling us to aggregate and rearrange simulation results for analysis.

Root Cause

Every event in our model originates from a root cause. By identifying and understanding root causes, we can quantify the impact of specific policy exclusions and endorsements on our overall portfolio.

We consider two possible root causes for an outage event: security failures and system failures. An example of security failure is if someone were to hack AWS and shut it down; an example of system failure is if an engineer at AWS inputs flawed code that causes it to shut down.

For a zero-day vulnerability event, the default root cause is security failure. An example is if hackers used an unknown vulnerability to attack a system, prompting other hackers to attack similar systems. In this case, a vulnerability in a widely used application or service could cause many security failures, all derived from the same vulnerability.

Aggregation Technologies & Vendors

Our event set includes eight cyber risk events that affect a specific ATV category. Because the underlying data is dynamic due to software updates and IT procurement decisions, we can stay ahead and reflect changes in digital technology and vendor usage in our analysis.

We use a simple, uniform distribution to pick ATVs from a larger category, so long as it meets a minimum threshold of detections among policyholders. Specific ATVs can be filtered out based on expert judgment. For example, we only simulate losses based on ATVs with a credible path to multiple compromises. Similarly, we might merge various variations of the same ATV.

Severity

To calculate event severity, we use bespoke severity components to connect event realizations with policyholder financial data. Depending on the event type, the severity component is based on either a static or deterministic percentage of the ground-up loss and applied on a basis most relevant to the type of cyber event.

We apply a static parameter that represents the percentage of business interruption — the most significant driver of loss for outage events — used to calculate ground-up losses. In the

event of a hosting outage, our model assumes 100% business interruption loss due to the nature of the event. However, in the event of an email outage, our model accounts for the fact that such an event wouldn't necessarily shut down an entire business.

Similarly, for a weaponized zero-day vulnerability cyber event, we apply a static parameter representing the total zero-day vulnerability severity factor used to calculate ground-up losses. Based on Coalition's loss history, the severity factor is a weighted average of event-specific severity components based on a blend of events that are significant drivers of loss, including ransomware and data compromise.

To separate technical modeling from the severity and cost component modeling, we also model sources of post-realization technical uncertainty with custom distributions and assumptions to account for extreme and irregular cyber events. We expressly model outage length for the different outage events and the proportion of policyholders impacted by a zero-day vulnerability event. We use an Inverse Gaussian distribution with a relatively heavy tail for outage events. For zero-day vulnerability events, Coalition's actual loss data for the losses that could occur from a zero-day vulnerability establishes the loss distribution.

Policyholder Details

To calculate insured losses, we use various elements of the insurance policy, such as terms and conditions, coverage, and endorsements, to determine the loss amount for affected policyholders and the loss amount for Coalition. We consider a systems failure variation for every outage event. Additionally, we use quota share information to calculate how simulated losses can impact Coalition's (re)insurance partners.

Model Results

To illustrate the capabilities of our Active Cyber Risk Model, we compiled a sample portfolio of fast-growing businesses in North America. Using Coalition's relevant digital data, we ran a 100,000-year Monte Carlo simulation against a catalog of catastrophic cyber events to estimate the potential impacts on the U.S. economy.

Spanning more than 35 distinct industries, the sample portfolio businesses collectively generate revenues of $318 billion (1.25% of U.S. Gross Domestic Product[1]). Below are the components used in this simulation:

- **Event Set**
  We used Coalition's standard event set, consisting of advertising outages, CDN outages, DNS outages, email outages, hosting outages, payments outages, SSL/TLS certificate provider outages, and software susceptible to zero-day vulnerabilities.

- **Frequency**
  We used Coalition's reference statistical distribution for rare events frequency.

- **Root Cause**
  We set the root cause of outage events to be an equal chance of security failure or system failure, while the default root cause of zero-day vulnerability events is security failure.

- **ATV**
  We scanned our sample portfolio to identify ATVs for every type of event in our eight-event set. Please note that the technologies and vendors we identified are not inherently risky. Instead, these ATVs are the most likely to lead to a catastrophic cyber event due to their widespread adoption among the businesses in our sample portfolio.

- **Severity**
  We based the severity component on revenue, industry, and type of loss.

Upon completion of a simulation, our model produces a Year Loss Table that contains all of the event realizations with various loss metrics for a given catalog of cyber events against a portfolio of policies. Based on this data, we generate a dashboard of reporting metrics that focus on different types of perils to help with portfolio cyber risk quantification and management.

1. *Estimations based on 2022 U.S. Gross Domestic Product.*
2. *All ATVs were identified by Coalition scans performed on January 17, 2023. The list provided should not be considered static, as new technologies regularly emerge among the businesses within a portfolio.*

Simulation ATVs by Event Type

Event Type	ATV
Advertising outage	AdRoll, Google AdSense, Xandr (AppNexus)
CDN outage	Amazon CloudFront, Cloudflare, Incapsula
DNS outage	Cloudflare, MikroTik, PowerDNS
Email outage	Microsoft 365, Google Workspace, SendGrid
Hosting outage	Akamai, Amazon CloudFront, Amazon Web Services, Microsoft Azure
Payments outage	Braintree, Stripe, PayPal
SSL/TLS certificate provider outage	Comodo, Digicerts, Globalsign
Software susceptible to zero-day vulnerabilities	AkamaiGHost, Amazon CloudFront (daemon), Amazon Web Services, Apache, Cloudflare, Nginx, Microsoft Internet Information Services, Microsoft 365

Average Annual Loss

Our model determined the average annual loss (AAL) for our sample portfolio to be approximately $10 million. These collective losses, which only consider catastrophic events and do not account for traditional cyber events like ransomware, business email compromise, and funds transfer fraud, directly result from shared ATVs.

Simulation by the Numbers

Event Realizations Across Simulated Years	Average Number of Events per Realization	Average ATV Hit Rate
2.25%	1.06x	9.42%

Drivers of Loss

Our model helps us understand which ATVs are the greatest contributors to AAL. Generally, we look for three vital characteristics:

1. ATV is widely used by policyholders
2. ATV is directly linked to policyholder profits
3. ATV is subject to compromise by failure at scale

This criteria enables us to identify the largest contributors to average losses and provide data-driven feedback loops to other business units. If these characteristics are true about a given ATV, we may consider taking additional action to manage our exposure to aggregate cyber risk.

For our sample portfolio, our model determined Cloudflare, Microsoft 365, and Amazon CloudFront were the ATVs that most contributed to AAL among our sample portfolio.

Top Contributors to AAL

ATV	Event Type	Contribution to AAL (%)
Cloudflare	CDN outage	20%
Microsoft 365	Email outage	13%
Amazon CloudFront	CDN outage	10%
Google Workspace	Email outage	5%
Nginx (webserver)	Software susceptible to zero-day vulnerabilities	3%
Microsoft 365	Software susceptible to zero-day vulnerabilities	2%
Microsoft Internet Information Services	Software susceptible to zero-day vulnerabilities	2%

CDN outages are a helpful example to illustrate because many businesses use CDNs and reverse proxies to host online assets, such as images, videos, or code. CDNs improve performance and reduce the latency to access an organization's assets for end users. CDN outages are also a frequent source of aggregate cyber risk due to the sheer number of organizations that depend on them to operate.

Individual businesses can be directly impacted in the event of a CDN outage. Those that rely on an online presence to generate revenue would likely experience lost income due to business interruption. News publications might be unable to generate page views on their website, while eCommerce businesses could see customers abandon their shopping carts — sometimes costing thousands, even millions, of dollars per minute.

CDN provider Fastly experienced an outage in 2021 that caused nearly an hour of downtime for some of the most popular websites in the world. Caused by a bug within one service provider, the outage brought down 85% of Fastly's network within five minutes. Similarly, Cloudflare experienced a CDN outage in 2022 that took 19 of its busiest data centers offline and downed websites for over an hour.

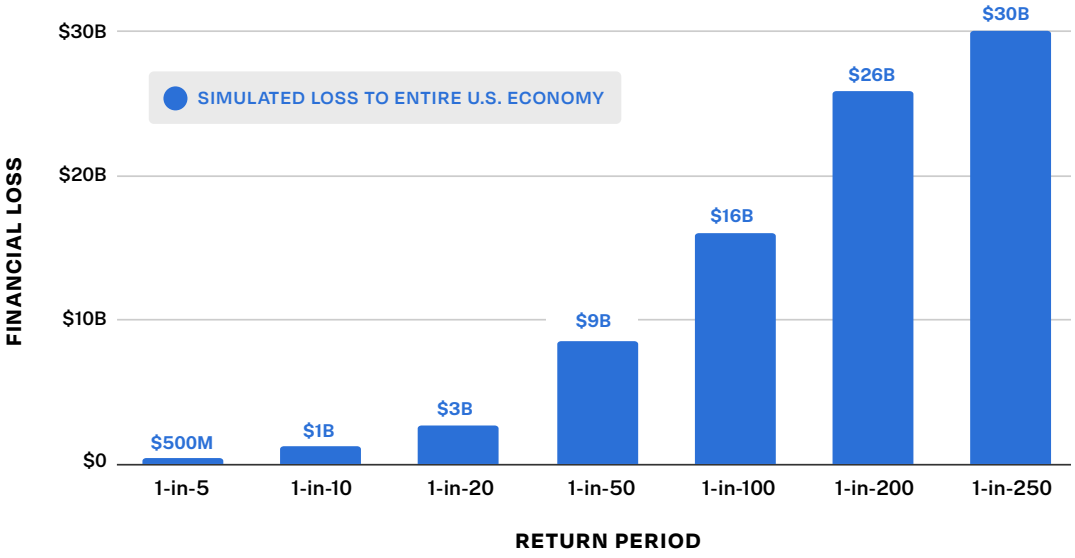
The Fastly event was a global outage, while the Cloudflare event was localized due to its unicast network architecture. Based on our model and understanding of network topologies and aggregate cyber risk, local CDN outages are more realistic and less impactful events, while widespread CDN outages are much less realistic but far more impactful.

Exceedance Probability

The loss distributions for rare events, such as catastrophic cyber events, are often highly skewed. To distill this information, we look at exceedance probabilities and return periods to determine the likelihood of exceeding a given loss level for various target return periods.

Financial Losses from Simulated Catastrophic Cyber Events

Return Period	Sample Portfolio	Entire U.S. Economy[3]
1 in 5-year loss	$6 million	$500 million
1 in 10-year loss	$15 million	$1 billion
1 in 20-year loss	$34 million	$3 billion
1 in 50-year loss	$107 million	$9 billion
1 in 100-year loss	$200 million	$16 billion
1 in 250-year loss	$372 million	$30 billion



For our simulation, 66% of the simulated years resulted in no financial losses for the sample portfolio. We calculated the following aggregate exceedance probability losses, then extrapolated those losses over the entire U.S. economy. Based on our model, a rare instance of catastrophic cyber events could cost American businesses an estimated $30 billion in total losses.

3. *Estimations based on 2022 U.S.Gross Domestic Product.*

Mitigating Cyber Risk with Active Insurance

Due to the nature of systemic cyber risk, we may never be able to prevent a catastrophic event itself from occurring. Even with the most sophisticated models and precise data, how such an event might occur seems forever out of our control. What is within our control, however, is how Coalition proactively works to mitigate the potential for widespread loss.

Active Insurance helps Coalition monitor and notify policyholders about emerging vulnerabilities to mitigate the potential for security failure. Our Active Risk Platform provides a comprehensive, near real-time cyber risk assessment for every new business when quoting an insurance policy, which allows us to improve the individual risk profiles of potential policyholders.

Importantly, our ability to reduce risks doesn't stop once a policy is purchased. We continuously monitor policyholders for ATVs and use personalized alerts to notify policyholders of new threats and provide actionable recommendations on how to mitigate their exposure — a crucial line of defense that can translate into immediate and material business impact in the event of a widespread cyber event.

Active Insurance also helps us manage exposure to aggregate cyber risk to mitigate the effects of system failure. Not only does monitoring ATVs enable us to make the best risk selections for our portfolio, but it also allows us to drive down or offset cyber risk using our insurance policies.

If a risk becomes too prevalent in our portfolio, we can use pricing adjustments to increase the cost of a policy, which would offset the increased risk from a financial perspective. By identifying and mitigating cyber risks pre-policy, we can help reduce the risks that can lead to catastrophic cyber events.

Active Insurance gives us the power to influence overall portfolio health and ensures that we remain aware of the most vulnerable points of aggregation, so we can take action before issuing a policy and throughout its lifetime.

Active Insurance gives us the power to influence overall portfolio health and ensures that we remain aware of the most vulnerable points of aggregation, so we can take action before issuing a policy and throughout its lifetime.

Bringing Stability to the Cyber Insurance Industry

An active approach to cyber risk management is the best way to keep pace with the ever-changing nature of the digital world. We protect policyholders by building tools to help mitigate risk and prevent attacks before they happen — and this approach works.

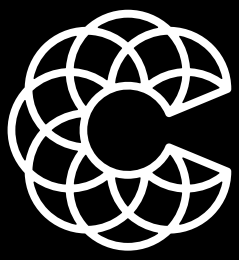
In 2022, Coalition policyholders experienced claims at a frequency 70% lower than the industry average.[4] Our continued success is supporting proof that cyber risk is insurable. In fact, with the correct data and knowledge, cyber risk is one of the most knowable risks in the modern world.

With deep insights and vast amounts of proprietary data, our Active Cyber Risk Model ensures we know where our cyber risk is aggregating within our portfolio, which means we know how much capital is needed to protect our policyholders. What separates Coalition from legal insurers is that we have the right tools and systems to measure cyber risk and reduce its impact on policyholders and our portfolio.

Our mission is to protect the unprotected. We live this mission daily by providing coverage to the organizations that need it, protecting them throughout the policy period, and helping them recover following incidents — all in the name of protecting businesses from cyber threats. All organizations need the peace of mind and protection afforded by a cyber insurance policy to operate efficiently and effectively, which is why cyber insurance will continue to play an essential role in the modern economy.

As insurance leaders, we are willing to stand up and support our assertion that cyber risk aggregation isn't an existential threat to the industry. Instead, Coalition remains confident that a practical framework and understanding of cyber risk aggregation can unlock sustainable underwriting models and bring stability to the cyber insurance industry.

4. Coalition, 2022 Claims Report: Mid-year Update.



Coalition®

coalitioninc.com

help@coalitioninc.com

55 2ND STREET, SUITE 2500
SAN FRANCISCO, CA 94105