Suite of Cyber Risk Models

Cyber risk is evolving and multifaceted; to help (re)insurance companies manage this risk, Verisk has developed a suite of tools that help you to quantify it. Each model can help your organization assess a different aspect of the risk; together, these models provide the most comprehensive view of potential cyber threats.

Verisk

As cyber risk continues to evolve, so too will our set of cyber solutions to provide you with the analytics you need to effectively manage your risk

Our suite of cyber risk models helps (re)insurers understand their loss potential to both individual cyber risks and aggregation cyber events before they occur. These data-driven models leverage machine learning and stochastic simulations to deliver insights about the likelihood of cyber incidents and the financial impact that those incidents could have on individual risks or books of business.

Individual Cyber Risk Models

Individual cyber event losses continue to dominate today's cyber claims and represent a real, material risk for (re)insurers. Individual cyber risk losses are driven by often smaller, more frequent losses that arise from single, potentially targeted, cyber events impacting individual insureds. Our individual cyber risk models probabilistically capture these losses across 8 of today's most prevalent event vectors: malicious breach, phishing/social engineering, physical tampering, lost or stolen devices, unauthorized access, unauthorized disclosure, unintentional disclosure, and cyber extortion.

Each event vector represents an avenue of loss that can be modeled across more than a dozen first- and third-party cyber coverages. These coverages extend across a comprehensive collection of today's standard market coverages, modeling losses across first-party breach response and crisis management, recovery of data and digital assets, as well as third-party damages. Using the individual cyber risk models enables (re)insurers to monitor losses arising from these types of events across the ever-evolving cyber risk landscape. Its flexible, transparent framework allows analysts to study the drivers of modeled loss and test their own views of risk. In addition, the model is calibrated with public, commercial, and insurance claims data on more than 77,000 worldwide cyber incidents and the cybersecurity profiles of 100,000+ organizations globally. Underlying the probabilistic model is our state-of-the-art Cyber Industry Exposure Database (IED), which features more than 12 million organizations across the globe.

You can leverage the models' unique abilities to differentiate risk to improve underwriting practices and identify the policy terms that deliver the best returns, while staying within your organization's risk tolerances.

Cyber Risk Aggregation Models

Cyber events impacting many insureds have the potential to generate extreme aggregate losses. The cyber risk aggregation models enable (re)insurers

to evaluate the impact of systemic cyber scenarios against their cyber book of business, looking to points of aggregation as sources of loss. Losses are captured both probabilistically and deterministically across an array of aggregate scenarios.

Provider Failures and Outages

The widespread adoption of cloud services has made providers of these services a major source of systemic risk that could cost the global economy billions in business interruption losses if a major downtime incident were to occur. Given that each cloud service provider in the market is a uniquely architected and independently managed business, insurers must go beyond simply tracking limits associated with each provider to understand the losses that can be expected from each. To meet this need, the model uses stochastic techniques to simulate downtime events for more than 100 different cloud service providers. Each unique event describes which cloud provider went down, the cause of the outage, the length of the downtime, and how many of the cloud provider's data centers were affected.

In addition to cloud service provider outages, the cyber risk aggregation models capture losses arising from the failure of other provider types, either deterministically or probabilistically, across 7 aggregation scenarios:

- Probabilistic and deterministic cloud/hosting provider downtime model
- Email outage
- Payment processor outage
- Ad provider outage
- Content Delivery Network (CDN) outage
- Domain Name System (DNS) outage
- Secure Sockets Layer (SSL) certificate failure

Systemic Ransomware Model

The systemic ransomware model focuses specifically on events that threaten the largest losses and are historically represented with such events as WannaCry and NotPetya. These events are partial-aggregation in that not every organization exposed to one of these worm-like ransomware threats will actually be impacted by the event. The model uses market share data and focuses on points of aggregation to understand the potential spread and severity of these events.

The systemic ransomware model is a probabilistic model with a 50,000-year event catalog of varying severities. Each event in the stochastic catalog looks across the following:

- Points of aggregation: A common set of criteria that must be met for successful infection and propagation, such as operating system, location of IT infrastructure, industry classification, unpatched vulnerabilities, etc.
- Propagation: The spread of an event, both within a company and across the internet. The systemic ransomware model accounts for industry trends and cybersecurity posture in assessing the spread—and ultimately severity—of an attack
- Severity: How many companies were impacted and how severe the disruption was based on the duration of downtime. The systemic ransomware model calculates company-specific downtime distributions that account for preparations such as backups and remediation plans; we also include industry-specific parameters that would make the same event result in higher or lower losses for some

The output modeled results capture losses across 4 key coverages: business interruption, data/asset recovery and remediation, forensics/incident remediation, and extortion.

Deterministic Scenarios

Aggregate cyber risk provides specific, non-variable results that depend directly on the provided inputs, as there is no inherent randomness. It uses the augmented detailed accumulation and market share approaches to calculate deterministic results across provider failure and outage deterministic scenarios.

By adjusting the underlying scenario conditions and retesting, you can measure the financial benefits and compare them with the cost of implementation and enforcement of specific mitigation tactics.

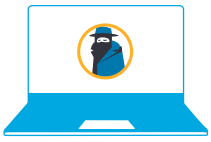
The deterministic scenarios use our Cyber Industry Exposure Database, as well as proprietary databases to assess the risk for both organization-based and property-based models.

Cyber Industry Exposure Database

Our comprehensive Cyber Industry Exposure Database underlies our suite of cyber risk models. This database represents the insurable global cyber market and contains firmographic and technographic information for more than 12 million organizations that can be used to augment your exposure data. When company-specific detailed data isn't available, our models can provide aggregated detailed data and produce industry- and region-specific market shares that can be applied to organizations across 7 market regions, including the United States, Canada, United Kingdom, Europe, Japan, Australia, and rest of world (RoW). Insurers can leverage this database to begin modeling cyber risk with as little information as the name of the organization or the organization's industry and revenue.

Cyber as a Peril

Most cyber risk is covered by an affirmative cyber policy, meaning that cyber risk is specifically covered via a standalone policy or an endorsement on a policy. Silent cyber coverage reveals itself when the impacts of cyber incidents are not explicitly included or excluded in the policy wording. Due to the potential for losses outside affirmative cyber lines, it's important to understand your exposure to this potential threat. Offered on a consulting basis, we can help you model your silent cyber risk so that you are prepared for even these potential losses.



Probabilistic Models at a Glance

- Modeled Incidents
  - Cyber incidents that lead to individual event losses through (un)correlated events, which include malicious breach, phishing/social engineering, lost/stolen devices, unintentional disclosure, physical tampering, cyber extortion, unauthorized access, and unauthorized data collection

  - Cloud/hosting service provider downtime
  - Systematic ransomware
- Model Domain: Global
- Catalog Size: 50,000 years
- Supported Insurance Coverages
  - 14 different coverage splits: call center costs, communication costs to regulators, credit/identity monitoring, crisis management, extortion, cyber forensics/incident remediation, funds transfer fraud, legal defense costs, notification costs to data breach victims, PCI & regulatory penalties and fines, public relations, data/asset recovery and reconstruction, third-party liability, and (contingent) business interruption
- General Data Protection Regulation (GDPR) fine estimates
- Industry Exposure Database
  - 12.4 million organizations globally
  - Company-specific technographic data and supply chain data for more than 100,000 companies
  - Region-specific industry market share data across different industry and revenue bins for the U.S., Canada, United Kingdom, Europe, Japan, Australia, and rest of world (RoW)
- Model Output
  - Average annual loss (AAL), exceedance probability losses, year loss tables (YLTs), event loss tables (ELTs) and the underlying metadata for each incident type
  - Event descriptions and top loss drivers
  - Exposure data on technographic attributes of modeled organizations, such as cloud provider usage
  - Sensitivity testing on cyber hygiene scores

Verisk's Cyber Solutions:

Verisk's cyber solutions offers a holistic view for managing cyber risk across the (re)insurance value chain. Built on a best-in-class industry database that contains firmographic, technographic, and policy information on more than 12 million businesses, Verisk's robust suite of cyber solutions helps (re)insurers address the challenges of today's cyber markets. www.verisk.com/cyber

About Verisk

Verisk (VRSK) is a leading data analytics provider serving customers in insurance, energy and specialized markets, and financial services. Using advanced technologies to collect and analyze billions of records, Verisk draws on unique data assets and deep domain expertise to provide first-to-market innovations that are integrated into customer workflows. Verisk offers predictive analytics and decision support solutions to customers in rating, underwriting, claims, catastrophe and weather risk, global risk analytics, natural resources intelligence, economic forecasting, and many other fields. Around the world, Verisk helps customers protect people, property, and financial assets. Headquartered in Jersey City, N.J., Verisk operates in 30 countries and is a member of Standard & Poor's S&P 500® Index. In 2018, Forbes magazine named Verisk to its World's Best Employers list. For more information, please visit www.verisk.com.