



RMS Cyber Accumulation Management System

Capture, store, and report on cyber exposure data within a standardized framework to manage cyber accumulation risk



KEY BENEFITS

- Standardized framework approach for capturing, identifying, and reporting cyber exposure
- Stress test portfolios using a range of catastrophic cyber scenarios
- Model probable maximum loss, risk accumulations, and correlations across a portfolio
- Quantify affirmative and silent cyber exposure policies
- Capture additional user-specific data for inclusion in accumulation reports
- Tailor view of risk by incorporating own research and claims data
- Produce correlated cyber analytics using accumulation engine, informing risk appetite, capacity, and capital requirements

Start to capture and quantify cyber risk

Cyber crime is widely acknowledged as one of the biggest threats facing businesses today. Mitigating this risk is quickly becoming a top business priority and represents a fundamental driver for growth in the global (re)insurance industry.

The RMS Cyber Accumulation Management System is the first to provide a framework for capturing and quantifying cyber risk, enabling the (re)insurance industry to maximize the opportunity afforded by this new and emerging peril.

A framework for identifying and managing cyber exposure

The RMS Cyber Accumulation Management System offers the capability to capture, store, and report on cyber exposure data within a standardized data framework. This system is underpinned by the RMS Cyber Exposure Data Schema, designed in collaboration with the University of Cambridge Centre for Risk Studies and a broad range of practitioners from across the industry. This provides a standardized approach for identifying, quantifying, and reporting cyber exposure.

The RMS Cyber Exposure Data Schema allows for the capture of five key categories of cyber exposure:

- Geographical Jurisdiction
- Cyber Loss Coverage Categories
- Business Sector
- Enterprise Attributes
- Cyber Risk Attributes

Using this data schema provides the common language and approach for understanding and measuring cyber accumulation risk, to facilitate a more streamlined risk transfer process.

Cyber loss process models to stress test your portfolio

RMS has created five loss process models developed to stress test a (re)insurer's portfolio. These models reflect five of the key IT-related cyber threats and represent severe but plausible examples of systemic cyber catastrophes.

RMS CYBER SERVICES PRACTICE

Our Cyber Services Practice offers a range of support and consultancy services to help you with cyber risk management, including:

- Installation, training, and support on the solution available from RMS cyber experts
- Silent and affirmative cyber exposure data reviews to support adoption of the RMS Cyber Exposure Data Schema
- Work together to develop your own view of risk in consultation with RMS
- Establish cyber risk management best practices by leveraging RMS cyber domain expertise
- Fully outsource your cyber modeling requirements to RMS

The models explore how correlated losses could impact large numbers of policies across a portfolio with the output enabling users to identify the key drivers of loss for each model.

The five loss process models are:

- Cyber Data Exfiltration—*Leakomania*
- Denial of Service Attack Loss—*Mass DDoS*
- Financial Transaction Compromise—*Financial Transaction Interference*
- Cloud Provider Failure Model—*Cloud Compromise*
- Extortion Incidence Model—*Extortion Spree*

In addition to the RMS view of the severity of these scenarios, the key levers that determine the severity of these events have been parameterized, allowing companies to incorporate claims data or other research to build their own view of the risk.

Flexible reporting engine

The accumulation engine provides a framework for analyzing exposure and loss results across both silent and affirmative cyber insurance policies. With out-of-the-box analytics to help support the understanding of accumulations of risk and key drivers of loss from within the scenarios, the accumulation engine provides the business insight required to set and monitor risk appetite over time.

Developed with leading industry experts

RMS developed the Cyber Accumulation Management System in collaboration with eight development partners representing a broad range of insurance industry perspectives, together with the University of Cambridge Centre for Risk Studies.

RMS

7575 Gateway Blvd.
Newark, CA 94560, USA

For sales inquiries:

+1.510.505.2500
+44.20.7444.7600
sales@rms.com

www.rms.com



Find out more

To find out more about the RMS Cyber Accumulation Management System, visit rms.com/cyber or send an email to cyberrisk@rms.com.



RMS is the world's leading catastrophe risk modeling company. From earthquakes, hurricanes, and flood to terrorism and infectious diseases, RMS helps financial institutions and public agencies understand, quantify, and manage risk.

©2016 Risk Management Solutions, Inc. RMS is a registered trademark and the RMS logo is a trademark of Risk Management Solutions, Inc. All other trademarks are property of their respective owners.