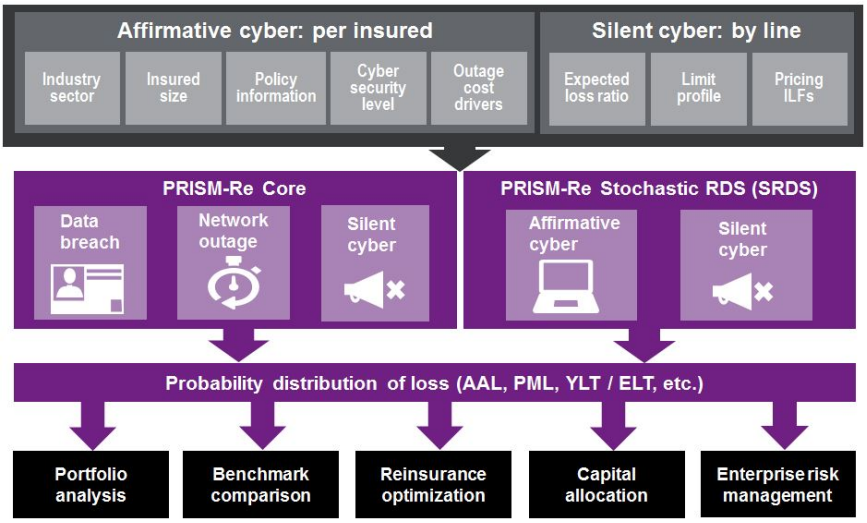
As our dependence on digital technology grows and cyber exposures permeate insurance risk across multiple lines of business, external stakeholders are demanding to know how insurers are measuring their exposure to cyber risk in all its forms, including losses in the tail. **Regulatory authorities such as the PRA in the UK now require insurers to systematically quantify and manage their broad exposure to cyber as a peril and this has helped promote the development of cyber catastrophe scenarios to stress test portfolios.** Cyber exposures are only going to grow and we see stakeholder involvement growing too. We have therefore extended the scope of **PRISM-Re** to assist our clients in measuring their exposure to cyber risk and support their broader risk and capital management strategies.



PRISM-Re Core vs. SRDS

PRISM-Re, the industry's first cyber portfolio management tool, quantifies both affirmative and silent cyber exposure stochastically utilizing two distinct models:

- **PRISM-Re Core** is a full probabilistic model, estimating attritional and systemic losses based on the analysis of historical cyber incidents, a proprietary claims database, published studies, and expert opinion.
- **PRISM-Re SRDS** projects extreme cat losses under defined Stochastic Realistic Disaster Scenarios based on a portfolio's exposure aggregation.

The two components are complementary: the **Core** model works bottom-up to generate losses for individual policies by reflecting their unique characteristics, while the **SRDS** module works top-down to quantify the impact of industry-level event losses on a specific insurance portfolio.

Applications of PRISM-Re Core & SRDS

- The **Core** model can be used to quantify a portfolio's cyber AAL and PMLs for both attritional and systemic exposure to affirmative and silent cyber.
- The **SRDS** module allows an insurer to evaluate how exposed its portfolio is under a set of defined extreme CAT scenarios which can be used for internal / regulatory reporting and stress testing.
- The data requirements to run PRISM-Re are **user-friendly** and easy to compile as the model examines exposure characteristics at a broad industry level.
- The model includes the ability to compare a cyber portfolio against **Willis Re's benchmark industry portfolio** which is comprised of >60k policies with nearly $1bn of gross written premiums.
- The model can also be used to evaluate a wide range of reinsurance structures in order to mitigate risk and manage net exposure.

PRISM-Re Core Affirmative cyber model

The affirmative cyber model comprises two separate modules: privacy breach and network outage.

Privacy breach module

Relying on comprehensive cyber threat intelligence and historical breach incident data licensed from Advisen, Willis Re performed detailed regression analysis to identify relationships between vulnerability to privacy breach and the insured's size and industry sector. Using the **rate of privacy breach** parameters, the module simulates years in which the portfolio is exposed to potential privacy breaches.

In each simulated breach, PRISM-Re generates a **number of records affected** and allocates the simulated records to different **data types**: PCI, PHI and PII, alongside estimating a cost for each data type based on proprietary claims data.

Network outage module

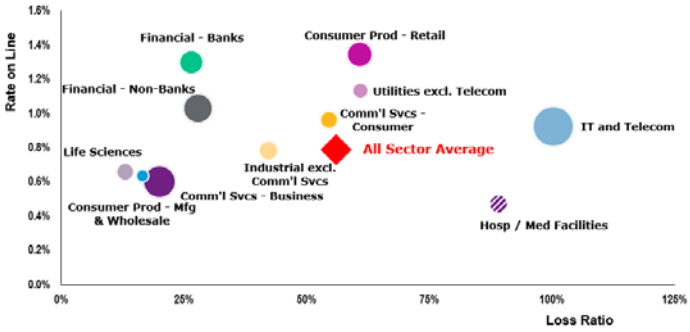
Parameters for the **rate and duration of network outage** were developed by combining the results of published studies with the expert opinion of Willis Towers Watson professionals and the views of specialists in leading companies from a representative mix of industries.

Each industry's potential vulnerability to "**black swan**" vs. "white swan" events was assessed as was the propensity for partial or total outages at various durations. Factors such as the insured's size and relative cyber security posture were also reflected.

For each hour of outage**,** the model estimates various categories of **outage costs**: cost of lost productivity and lost income, as well as costs of data and/or system restoration.

Industry Benchmark

Cyber insurers can compare key metrics such as ELR, ROL, sector concentration, etc. from their own portfolio against Willis Re's robust cyber industry database.

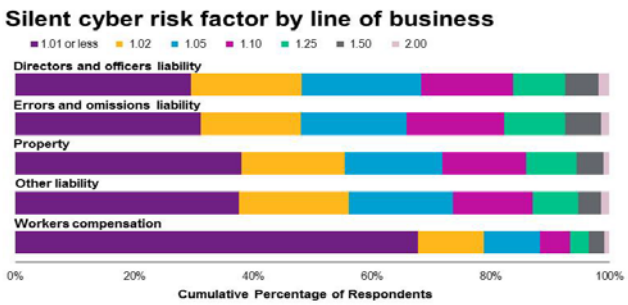


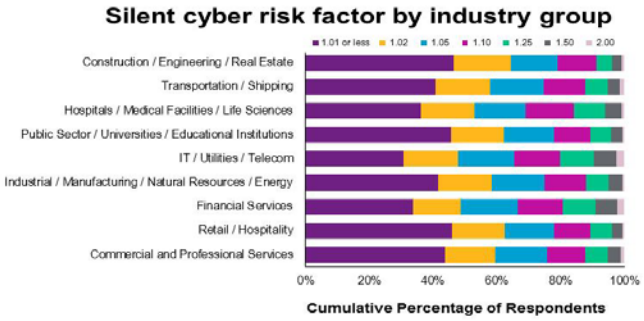
PRISM-Re Core Silent cyber model

The silent cyber model is designed to address insurance companies' exposure to silent cyber – cyber risk exposure that is neither affirmatively granted nor specifically excluded.

The model deploys an exposure rating approach to quantify a company's silent cyber loss potential. It incorporates the **likelihood of a claim resulting from silent cyber** with client-specific **non-cyber limits profiles and loss severity curves** to generate a full loss distribution of silent cyber in isolation, or in conjunction with affirmative cyber loss.

The silent cyber frequency component is derived from the responses of around 700 insurance professionals to Willis Re's 2018 silent cyber survey that focused on the extent to which cyber exposure would increase the likelihood of a claim to various industry segments in five major commercial lines (property, other liability, D&O, E&O, and workers compensation).



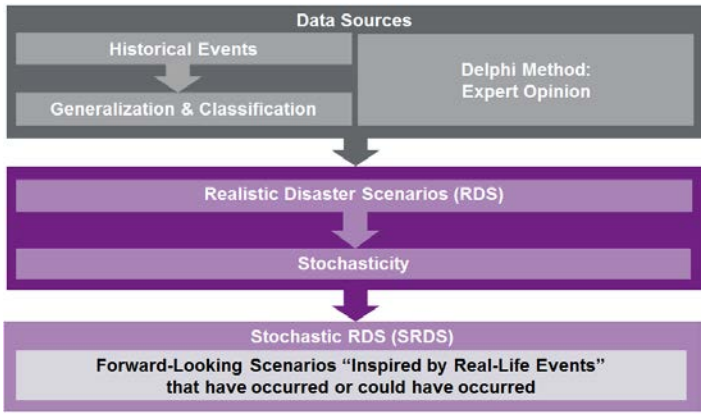


Core Systemic Loss potential

Both the Affirmative and Silent cyber models contemplate the potential systemic impact of cyber events. The Affirmative model assesses the possibility of within/across industry sector clustering via a common shock matrix while the Silent module implements this across the lines of businesses via a correlation copula. Both methods are transparent and customizable.

PRISM-Re SRDS cyber CAT model

Realistic Disaster Scenarios are a practical, intuitive, exposure-based approach to quantifying casualty catastrophe. **PRISM-Re Stochastic RDS** applies forward-looking cyber CAT scenarios to a company's portfolio to estimate loss potential for each event and in total.



Given the evolving cyber threat landscape, the model's extensive catalog of RDS's is inspired by representative cyber CAT events in history and at the same time reflects potential scenarios that may happen in the future.

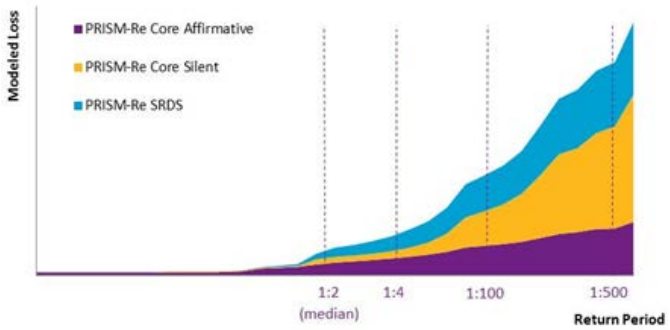
Historical Loss Example	Inspired Scenario	Affirmative vs. Silent?	Single vs. Systemic?
WannaCry NotPetya	Hacking/Network Outage	Silent	Systemic
German Nuclear Plant German Steel Mill	Industrial Hack - Utilities/Manufacturing	Silent	Single
Sweden DDoS Attack Poland Train Derailment	Industrial Hack - Transportation	Silent	Single
Ukraine Grid Sabotage	Blackout	Silent	Single
Target/Anthem Breach	Mass Data Breach	Affirmative	Systemic

PRISM-Re SRDS goes beyond deterministic scenario modeling by building in variability around key model parameters to produce stochastic outputs such as Event Loss Tables and comprehensive Exceedance Probability Curves.

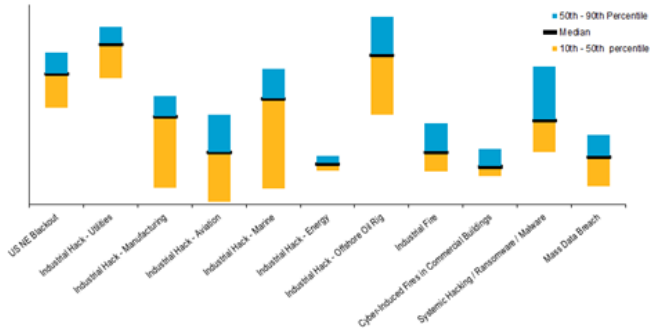
PRISM-Re v4

Key model outputs

Fully probabilistic modeled loss distribution



Scenario-based modeled loss comparison



Key model enhancements

1. Integration of SRDS scenario-based CAT model into PRISM-Re framework
2. SME-specific view calibrated to historical profitability of the segment
3. Updated and expanded industry exposure database with added benchmarking capabilities
4. Full breach parameter refresh
5. Enhanced common shock matrix to better reflect systemic impact
6. New 2018 Ponemon international cost per record relativities
7. Added ability to incorporate per-claim deductibles and limits

Contact us

Jess Fung
Willis Re Inc.
600 University Street, Suite 3100
Seattle, WA 98101
D +1 206 343 6066
E jess.fung@willistowerswatson.com

Mark Synnott
Willis Re Inc.
233 South Wacker Drive, Suite 2000
Chicago, IL 60606
D +1 312 774 1948
E mark.synnott@willistowerswatson.com