CYBER MODELLING

The evolution of cyber cat modelling

The strides made in model customisation will continue to dominate the conversation, say Guy Carpenter's Erica Davis and Anthony Cordonnier.

As the cyber market steps further into the limelight of the insurance industry, a flurry of risk developments has supported the growth and evolution of the products, players and sustainability of the market. Cyber catastrophe model vendors are vocal in the conversation, although as the 2024 turbulent loss landscape has highlighted, out-of-the-box modelled results may not sufficiently capture the scope and magnitude of emerging cyber cat losses.

Cyber cat models have had to scale rapidly against an evolving backdrop of perils, with a very limited event dataset to calibrate models and industry loss quantum. In less than 10 years, the market has progressed from no cyber-dedicated models to three robust options that offer unique toolsets and views of risks. The lack of historical event sets has likely influenced the significant variability among vendors, as each tackles the unknowns of the market through unique model infrastructures, independent assessments of the threat landscape and diverging views of the potential tail loss.

> "The CrowdStrike footprint was not directly modelled by any of the leading vendors."

"Kitty cat" years—periods marked by events that meet the criteria for a cat loss, but at a smaller scale—such as 2024 offer the market and models the opportunity to refine modelling methodologies and adjust views of risk away from expert judgement and towards empirical data.

The CrowdStrike outage in July highlights the gaps between modelled loss scenarios and actual loss experienced by the insurance market. In post-event analysis, the CrowdStrike footprint was not directly modelled by any of the leading vendors. As a result, some vendors released an "event track" approach shortly thereafter to facilitate an approximation of the event and address modelling limitations.

KEY POINTS:

- Cyber modelling is evolving
- An "event track" approach can help
- Post-event analysis drives model customisation

This approach attempted to help capture the nuance between malicious and non-malicious outages and how various coverage components might respond differently, depending on the loss vector. As an emerging peril, there is recognition that cyber events may not be perfectly parameterised in a model scenarios catalogue. Consequently, in the wake of systemic events, the market must work to reconstruct an event track from the pieces of various permutations.

Adjust and customise

Widening the scope of scenario analysis and event recreation, there is growing awareness of how to customise the models to more accurately match the risk profile of the underlying portfolio. Specialist cyber writers, whose books are not a perfect cross-section of the market, are finding they must adjust vendor model outputs to reflect the impacts of underwriting segmentation and security controls.

This is especially prevalent in the small and medium-enterprise (SME) revenue bands for which current vendor models are unable to accurately reflect the divergence in security posture between purchasers of insurance and the uninsured. This data capture challenge and lack of granularity in SME security differentiation may lead to overstatement of modelled cat losses.

SME specialists are currently collaborating with model vendors to refine how their models capture and reflect the impacts of fundamental security controls such as multi-factor authentication and endpoint detection and response to more accurately represent the true exposure for these carriers. Loss activity assessment and post-event analysis will help refine these assumptions further and drive model customisation, ultimately allowing niche writers to better reflect the merits of their portfolio.

Guy Carpenter is at the forefront of working with cedants, capital providers and model vendors to solve the current limitations in cyber modelling and better represent a bespoke view of risk. Cyber will remain a complex line of business that is changing rapidly in the face of an uncertain threat landscape.

> "Cyber modelling capabilities will evolve with the availability of improved datasets."

As global penetration rates increase, data capture becomes more granular and loss activity continues, cyber modelling capabilities will evolve with the availability of improved datasets—but the strides made in model customisation will continue to dominate the conversation through the re/insurance market's next act. ●

Erica Davis is global co-head of cyber at Guy Carpenter.

Anthony Cordonnier is global co-head of cyber at Guy Carpenter.