Cyber cat modeling innovates to overcome limitations

Customization and collaboration can help to address gaps in cyber modeling outputs, according to Guy Carpenter's Erica Davis and Anthony Cordonnier

In the last decade, cyber insurance has captured significant attention across the industry owing to its unprecedented growth rate, triple-digit rate increases and frequent headlines around evolving threats.

A wide range of risk quantification products, such as third-party vendor cyber catastrophe models, have been developed to support the growth, evolution and long-term sustainability of the cyber insurance market. However, as 2024's turbulent loss landscape has highlighted, out-of-the-box modeled 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 data set to calibrate models and validate their industry loss estimates. In less than 10 years, the market has progressed from zero cyber-dedicated models to three robust options that offer unique toolsets and views of risks.

> **Out-of-the-box modeled results may not sufficiently capture the scope and magnitude of emerging cyber cat losses**

The lack of credible historical event sets has likely influenced the significant variability among vendors, as each tackles the unknowns of the market through a unique methodology and modeling approach, independent assessments of the threat landscape and diverging views of the potential tail loss. "Kitty Cat" events in 2024 (cyber incidents that meet the criteria for a cat loss, but at a smaller scale) offer the market and vendors the opportunity to refine modeling methodologies and adjust views of risk away from expert judgment and toward empirical data.

The CrowdStrike outage in July this year highlights the gaps between modeled loss scenarios and actual loss experienced by the insurance market. In post-event analysis, the CrowdStrike event footprint was not comprehensively modeled by any of the leading vendors, as they lack true visibility into higher-degree dependencies within the digital supply chain, and their models do not contemplate a non-malicious event that is directly associated with CrowdStrike. Shortly after the outage, some vendors released an "event track" approach to enable an approximation of the event loss and solve for modeling limitations. As an emerging peril, there is recognition that cyber events may not be perfectly captured in a model scenario catalog. Consequently, in the wake of actual cyber events, the market must work to refine or expand the scope of the cyber catastrophe modeling framework.

Another aspect of continued model enhancement focuses on the customization of cyber models to more accurately reflect the underlying portfolio's risk profile. Specialist cyber writers, whose books are not a perfect cross-section of the market, are increasingly adjusting vendor model outputs to represent the impacts of underwriting segmentation and security controls, such as multi-factor authentication and endpoint detection and response. This is especially prevalent in the small and medium-sized business (SMB) segment, for which current vendor models are unable to account accurately for the disparity in security posture.

This data-capture challenge and lack of granularity in SMB security differentiation may lead to overstatement of modeled cat losses. Many niche cyber writers are currently collaborating with model vendors to refine their model assumptions through loss-activity assessment and post-event analysis, with the ultimate goal of better reflecting the unique characteristics and merits of their portfolios.

Looking across the current cyber threat landscape, new and resurgent risks – including business email compromise, generative AI and emerging privacy and biometrics regulations – all have the potential to lead to an escalating claims environment in a complex line of business. Guy Carpenter is committed to working with cedants, capital providers and model vendors to track these rapidly evolving cyber risks closely, solve for the current limitations in cyber modeling and better represent a bespoke view of risk. As cyber insurance penetration rates increase, data capture becomes more granular and loss activity continues, cyber modeling capabilities will improve over time – but the strides made in model customization will continue to dominate the conversation through the (re)insurance market's next act.

Erica Davis, global co-head of cyber, Guy Carpenter; Anthony Cordonnier, global co-head of cyber, Guy Carpenter