Cooley

Improving Cyber Insurance Practice Should Be a Company’s Priority

February 16, 2021

The New York State Department of Financial Services recently issued guidance for New York-regulated property and casualty insurers to effectively manage the cyber insurance risk present in their insurance portfolio. The DFS’ guidance signals an effort to reduce overall volatility in the cyber insurance market, which has been compounded by the recent proliferation of cyberattacks and by insurers’ widely varying approaches to measuring each policyholder’s cyber risk profile.

Although the DFS’ Cyber Insurance Risk Framework applies primarily to New York-regulated property and casualty insurers that write cyber insurance, the framework cautions that insurers that do not write cyber insurance nevertheless should evaluate their potential exposure to “silent risk” in their non-cyber insurance policies. Further, as the DFS has taken the lead in recent years among insurance regulators on cybersecurity issues, the framework provides valuable guidance to insurers that operate in states other than New York.

The framework’s guidance is divided into seven broad categories.

1. **Measuring aggregate cyber risk**. The framework advises that insurers establish a formal cyber insurance risk strategy for measuring this risk. This strategy should include clear qualitative and quantitative goals for cyber insurance risk, and such strategy should be directed and approved by the insurer’s senior management and board.
2. **Address potential cyber risk in “traditional coverages”**. The framework cautions that insurers should manage and eliminate exposure to silent cyber insurance risk. Although traditional insurance policies may not be intended to cover cyber risk and never even explicitly mention cyber, the wording of a policy nevertheless may be interpreted to cover loss from a cyber incident. The framework advises insurers to eliminate or mitigate this silent risk by revisiting the language of traditional policy forms as well as potentially purchasing adequate reinsurance coverage to hedge against this silent risk.
3. **Measure systemic cyber risk**. The framework recommends that insurers regularly evaluate systemic risk and plan for potential losses. Systemic risk is present in interconnected systems, in which an intrusion in one part of the system can create a domino effect to threaten all connected systems. The framework explains that insurers’ greater reliance on third-party institutions and vendors in recent years has increased systemic risk. These entities are prime targets for cyberattacks, and diversifying those institutions and vendors used will help mitigate the consequential impact of an attack on any single one. Further, the framework advises that insurers should regularly conduct internal cybersecurity stress tests to measure the fallout from potential catastrophic cyber events.
4. **Data-driven cyber underwriting**. The framework counsels that insurers should have a “data-driven, comprehensive plan” that evaluates the cyber risk of each policyholder and potential policyholder. Such plan should include details that enable the insurer to evaluate gaps in the policyholder’s cybersecurity measures, which can lead to better-informed pricing and improve knowledge about ways to enhance cybersecurity.
5. **Incentivize strong cybersecurity**. The framework recommends that insurers educate their policyholders and insurance producer partners about the value of strong cybersecurity measures and should incentivize

the adoption of these measures by pricing policies based on their effectiveness. Insurers are uniquely positioned to help incentivize strong cybersecurity practices by leveraging the cost of the protection afforded under their policies.

6. **Utilize cybersecurity experts to understand risk**. Insurers should hire cybersecurity experts and, as necessary, supplement these employees with additional consultants or vendors. The goal is to improve insurers' ability to forecast cyber exposures so they are acting proactively and not reactively.
7. **Law enforcement notification**. The framework advises that cyber insurance policies include a requirement that victims of a cyber incident notify law enforcement. Often, cyberattacks against multiple victims have a common origin, and notifying law enforcement can help to ensure that all possible victims are informed before extensive damage is done.

The DFS framework sends a clear message that increasing stability in an often-volatile cyber insurance market requires a collective effort among all parties. Promoting more informed underwriting, better cybersecurity practices and diversification of third-party institutions and vendors can help mitigate the frequency and impact of cyber events. Indeed, uninformed assessments of policyholders' cyber risk profiles or mispricing of cyber insurance coverages can potentially lead to more claims, reduction in the market's capacity, insurer insolvency and a greater appetite to deny covered claims.

Accordingly, policyholders and insurers alike should carefully examine their coverages in light of the DFS' directive – and in particular – assess the potential for provisions that cloud the intended coverage or create ambiguities affording silent cyber coverage. Counsel can assist with evaluating these issues and exploring creative solutions to mitigate the impact of cyber events. As cyberattacks are no longer an issue of *if* but *when*, mitigating cyber exposure should be top-of-mind for all stakeholders, large and small.