CYBER UPDATE

VENBROOK INSURANCE SERVICES

New York Issues Guidance for Insurers Writing Cyber Policies

As cybersecurity threats become increasingly sophisticated—contributing to a significant surge in cyberattack frequency and severity across the country—the New York Department of Financial Services (NYDFS) recently debuted a resource for insurers to utilize when writing cyber insurance. This resource, titled the Cyber Insurance Risk Framework, outlines best practices for New York-regulated property and casualty insurers in regard to analyzing policyholders' cyber risks and minimizing cyber-related losses.

The NYDFS explained that this resource was developed through engagement with insurance industry stakeholders and cybersecurity experts, and is intended to help insurers throughout the state of New York more effectively manage their cyber insurance risks. Although the NYDFS emphasized that every insurer's cyber risks will differ based on a range of factors (e.g., insurer size, market share, geographic distribution, resources available and industries insured) and insurers should adopt an approach that is proportionate to their unique exposures, the Framework encourages the following general best practices:

- **Create a formal strategy.** Insurers that offer cyber coverage should develop a formal strategy for properly measuring cyber insurance risks. This strategy should contain both quantitative and qualitative methods for identifying risks, and be approved by senior management, a board of directors or a governing body.
- **Address silent cyber risks.** Also known as non-affirmative cyber concerns, silent cyber risks refer to cyber exposures contained within standard commercial property and liability policies that don't specifically include or exclude cyber incidents. The ambiguity in these policies can allow insureds to misinterpret the extent of coverage provided, resulting in unexpected underwriting losses for traditional insurance carriers who didn't anticipate offering protection for cyber incidents or design their policies with cyber exposures in mind. Insurers can minimize silent cyber risks by establishing clear policy language and coverage conditions related to cyber incidents.
- **Consider systemic risks.** In response to the large-scale SolarWinds cyberattack in 2020, the insurance industry has become increasingly aware of systemic cyber risks, which refer to a policyholder's supply chain cybersecurity exposures. Moving forward, insurers should be fully aware of the third-party vendors used by their policyholders and conduct internal stress tests to determine cyber-related losses that could arise from insureds' supply chains.
- **Adequately measure policyholders' exposures.** To properly understand insureds' cyber risks, insurers should require detailed cybersecurity documentation—such as cyber incident response plans, workplace policies, access control and encryption protocols, boundary defense strategies and software security features—from each policyholder. This information, alongside past claims data, should allow insurers to identify potential gaps and vulnerabilities within policyholders' cybersecurity regimens.

- **Educate and reward policyholders.** Apart from examining policyholders' cybersecurity exposures, insurers should also educate insureds on how to prevent cyber incidents (and subsequent losses) from occurring. This may entail providing information on top cyber protection measures, giving access to various cybersecurity services or conducting workplace cyber assessments to determine how insureds can bolster their efforts. In addition, insurers should consider offering coverage incentives (e.g., policy discounts) to policyholders who integrate this education into their cybersecurity programs.
- **Hire cybersecurity experts.** Insurers that provide cyber coverage should make it a priority to recruit and hire employees with adequate cybersecurity experience, knowledge and skills. Including cyber experts within their workforce will allow insurers to better understand and assess policyholders' cyber exposures.
- **Require incidents to be reported.** Lastly, insurers should make sure that their cyber policies require insureds to notify law enforcement in the event that a cyber incident occurs. Doing so can help minimize the damages that result from a cyber incident, motivate law enforcement to prosecute the perpetrators, keep communities informed on current cyber threats and prevent future cybercrimes.

For additional industry updates and insurance solutions, contact us today.