HINSHAW

Alerts

New NYS DFS Cyber Insurance Risk Framework Warns Against Ransom Payments, Includes Notice to Law Enforcement Policy Requirement

February 8, 2021
Insights for Insurers: Cyber Coverage

The New York State Department of Financial Services (DFS) has issued guidance imposing rigorous cyber risk measurement and management practices on NY-regulated property/casualty insurers that write cyber insurance. The guidance also recommends against insurers making ransomware payments, noting recent FBI warnings and OFAC guidance that insurers can be held liable for ransomware payments to sanctioned entities. The framework also provides that cyber insurance policies should include requirements that victims notify law enforcement in the event of an attack.

After engaging in extensive dialogue with the insurance industry, cyber insurance experts and other stakeholders across the US and Europe, DFS developed a Cyber Insurance Risk Framework to foster more effective management of cyber insurance risk and bolster the industry. DFS points to the systemic risks faced by the insurance industry as a result of the proliferation and severity of cybersecurity attacks including ransomware. DFS cites to data indicating that from early 2018 to late 2019 the number of insurance claims related to ransomware increased by 180%, and the average cost of a ransomware claim rose by 150%. The number of ransomware attacks reported to DFS subsequently almost doubled in 2020 from the previous year; and the global cost of ransomware in 2020 was approximately $20 billion. The guidance letter also emphasizes “silent risks” posed by insurers having to cover cyber incident losses under policies that do not explicitly grant or exclude cyber coverage. Policies tied to errors and omissions, burglary and theft, general liability and product liability insurance can all carry this risk, DFS noted.

To more effectively confront these risks and build a more robust cyber insurance market, the Cyber Insurance Risk Framework requires that NY-regulated property/casualty insurers establish a board-directed strategy to measure and manage their cyber insurance risk, incorporating these specific best practices:

- Manage and eliminate exposure to “silent cyber” insurance risk
- Evaluate systemic risk, including the impact of catastrophic cyber events on third party service providers
- Rigorously measure insured risk by using a data-driven approach to assess potential gaps and vulnerabilities in an insureds’ cybersecurity

Service Areas

Privacy, Security & Artificial Intelligence

Regulatory and Compliance Counseling

- Educate insureds and insurance producers about the value of cybersecurity measures and the need for, benefits of, and limitations to cyber insurance
- Obtain cybersecurity expertise through strategic recruiting and hiring practices
- Require notice to law enforcement in the event of a cyber attack.

Final Thoughts

The DFS Framework focuses on areas that have been of prime concern for insurers over the past several years, particularly the issues of systemic risk and aggregation and non-affirmative or silent cyber coverage. Moreover, primarily because of escalating ransomware remediation costs and payments, industry experts have reported increased underwriting scrutiny and a likely hardening of the cyber insurance market. Experts are hopeful, however, that the heightened focus on cyber and privacy risks will lead more policyholders to take advantage of the proactive risk management tools and services offered by many cyber insurers, which are designed to reduce the chances of an event happening in the first place, and minimizing the impact if one does occur.