NYDFS Announces Cyber Insurance Risk Framework to Address Increasing Cyber Risk

By: Gregory S. Capps and Linda D. Perkins
Insurance Industry Alert
2.5.21

Even if your company does not report to the New York Department of Financial Services (DFS), all insurers should heed warning to prepare for future cyber risk regulations and requirements. Cyber risk is real and has the potential to be catastrophic, if not sufficiently identified and addressed.

On February 4, 2021, DFS issued a letter to all authorized property and casualty insurers in a renewed effort to address increasing cyber risk for all organizations. The letter notes that the "COVID-19 pandemic has shifted more of our work and lives online, and this shift has introduced new vulnerabilities that cybercriminals are aggressively exploiting." In response, DFS has created a Cyber Insurance Risk Framework after consultation with industry representatives, cybersecurity experts and other stakeholders to address new and significant emerging systemic cyber risks, such as the hack of SolarWinds Orion Platform. The hack of SolarWinds disclosed a massive cyber vulnerability that continues to unfold in terms of the extent to which data security has been compromised in critical U.S. government agencies as well as multi-national companies, U.S. businesses and other organizations.

The letter also acknowledges that "insurers often incur losses from cyber incidents in insurance policies that do not explicitly grant or exclude cyber coverage – so-called 'non-affirmative' or 'silent' risk [that] even insurers that write little or no cyber insurance need to measure and manage . . . in their non-cyber insurance policies." Failure to sufficiently identity and address an insured's cyber risk only increases cyber risk in the long run and the cost of the breach cleanup that will largely be borne by the insurer. Cyber insurers should also be mindful of their obligations to report demands for ransom payments by cybercriminals as explained in advisories issued by the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) in the U.S. Department of the Treasury on October 1, 2020.

The Framework includes seven areas for attention:

1. establish a formal cyber insurance strategy that includes clear qualitative and quantitative goals for risk and reporting to senior management or board level officers and directors on progress against those goals for risk;
2. manage and eliminate exposure to silent cyber insurance by identifying non-affirmative cyber risk in policies and making clear policy statements as to what cyber insurance coverage is included and excluded;
3. evaluate systemic risk on a regular basis, including risk associated with an insured's use of third party vendors to conduct business operations;
4. rigorously measure insured risk by evaluating the maturity and vulnerabilities of an insured's cybersecurity program;
5. educate insureds and insurance producers about cybersecurity risks, mitigation and prevention as well as the benefits and limitations to cyber insurance, including policy limits and other monetary limits;
6. obtain cybersecurity expertise; and
7. require notice to law enforcement.

We will continue to monitor and report on these and other developments involving the insurance industry and cyber issues.

The members of our Insurance Industry Group and Cyber Law and Data Protection Team are available to discuss with you any questions you may have about how to make sure your business or company can work towards identifying and addressing cyber risk and policy coverage. For additional information or if you have any questions, please contact Gregory S. Capps (cappsg@whiteandwilliams.com; 215.864.7182) and Linda D. Perkins (perkinsl@whiteandwilliams.com; 215.864.6866).

This correspondence should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only and you are urged to consult a lawyer concerning your own situation and legal questions.