PUBLICATION

U.S.'s First Cyber Insurance Risk Framework Issued by New York Department of Financial Services

Authors: Matthew George White, Alexander Frank Koskey, III
February 12, 2021

New York remains extremely active in the cybersecurity and data protection arena. As we have recently discussed, New York is considering a proposed privacy bill that would greatly enhance consumer privacy rights, increase business obligations, and create new litigation/enforcement exposure. Meanwhile, the New York Department of Financial Services (NYDFS) has recently filed its first Cybersecurity Regulation enforcement action (analyzed here), required regulated entities to formally notify the NYDFS if they were directly impacted by the SolarWinds incident (discussed here), and has now issued the nation's first Cyber Insurance Risk Framework (Framework).

The Framework applies directly to all property/casualty insurers registered with the NYDFS, but will have wide-reaching effects on all businesses as they evaluate and purchase cyber insurance.

The stated goals of the Framework are to facilitate the continued growth of a sustainable and sound cyber insurance market by outlining best practices for managing cyber insurance risks. Not only are insurers writing cyber insurance obligated to follow the Framework's guidance, but all insurers need to evaluate their "silent risk" – i.e., the risk that an insurer must cover losses from a cyber incident under a policy that does not explicitly grant or exclude cyber coverage – and take steps to reduce that exposure. The Framework also advises cyber insurers that the NYDFS recommends against making ransomware payments and reminds insurers to be mindful of their obligations to report demands for ransom payments by cybercriminals as explained in recent advisories issued by FinCEN and OFAC (analyzed here).

The Framework comes as the cyber insurance market is exploding. In 2019, the cyber insurance market was $3.15 billion and it is estimated that by 2025 it will be over $20 billion. At the same time, organizations are facing increased cyber risk as cybercrime is becoming more common, more sophisticated, and more costly.

This alert will summarize key elements of the Framework.

The Framework requires all insurers to sustainably and effectively manage their cyber insurance risk. While noting that each insurer's risk will vary based on many factors including size, resources, geographic distribution, market share, and industries served, the Framework requires all insurers to review its best practices and take an approach proportionate to its risk.

The Framework identifies the following best practices:

- **Establish a formal strategy for measuring cyber risk**. The strategy should be directed and approved by senior management and the board/governing body and should include clear qualitative and quantitative goals for risk.

- **Manage and eliminate exposure to silent cyber insurance risk**. Insurers should eliminate silent risk by making clear in any policy that could be subject to a cyber claim whether that policy provides or excludes coverage for cyber-related losses. Because this process may take time, insurers should

mitigate existing silent risk, such as by purchasing reinsurance.

- **Evaluate systematic risk**. Insurers that offer cyber insurance should regularly evaluate systemic risk and plan for potential losses. This evaluation should include stress testing based on realistic catastrophic cyber events.

- **Rigorously measure insured risk**. Insurers should have a data-driven, comprehensive plan for assessing the cyber risk of each insured and potential insured. This process should include gathering information on the insured's cybersecurity program and assessing a multitude of topics like incident response planning, third-party security policies, vulnerability management, and corporate governance and controls.

- **Educate insureds and insurance producers**. Insurers should offer comprehensive information about the value of cybersecurity measures and facilitate the adoption of those measures. Insurers should also incentivize the adoption of better cybersecurity measures by pricing policies based on the effectiveness of each insured's cybersecurity program. Insurers should also educate insurance producers to have a better understanding of potential cyber exposures, types and scope of cyber coverage offered, and monetary limits in cyber insurance policies.

- **Obtain cybersecurity expertise**. Insurers should recruit employees with cybersecurity experience and skills and commit to their training and development, supplemented as necessary with consultants or vendors.

- **Require notice to law enforcement**. Cyber insurance policies should include a requirement that victims notify law enforcement when a cyberattack occurs.

Not only should all insurers pay attention to the Framework's requirements, including those related to ransomware payments, but businesses should also review the Framework as they consider their cyber insurance needs. The Framework has the potential to alter numerous aspects of cyber insurance coverage, including the areas identified above that have been a prime concern for insurers for years.

If you have any questions regarding the Framework, your cyber insurance policy, or any other aspect of your privacy policies and procedures, please contact the authors Matt White, CIPP/US, CIPP/E, CIPM or Alex Koskey, CIPP/US, CIPP/E, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.