Akin®

New York Department of Financial Services Proposes New Cybersecurity Regulations

Sep 20, 2016

Reading Time : **1 min**

By: Natasha G. Kohne, David S. Turetsky, Visiting Professor, College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University of Albany

The proposed regulation would also require the adoption of a written cybersecurity policy that addresses not only traditional network security and controls like encryption and multifactor authentication, but also:

- business continuity and disaster recovery planning and resources
- capacity and performance planning
- systems operations and availability concerns
- systems and network security and monitoring
- systems and application development and quality assurance
- physical security and environmental controls
- customer data privacy
- vendor and third-party service provider management (which themselves are required to have minimum cybersecurity practices and be periodically assessed at least annually)
- risk assessment
- incident response.

While the specificity in the draft regulation provides a useful road map for firms looking to bring their policies up to date, it also underscores the need for institutions to ensure that unwritten or informal policies, even where followed rigorously, are properly documented. The current draft also broadly defines “nonpublic information” that must be protected by

encryption to include “any information that can be used to distinguish or trace an individual’s identity.”

The regulation also requires that a firm’s cybersecurity policy be implemented by a designated Chief Information Security Officer who reports at least biannually to the board of directors on certain designated topics, including breach reports and the remediation of deficiencies. Significantly, the regulations require that the DFS be informed of any material breaches within 72 hours of their discovery.

While the Securities and Exchange Commission has monitored and enforced cybersecurity at registered investment advisers since 2014 through its Office of Compliance Inspections and Examinations, this represents a significant step by the DFS to regulate the cybersecurity policies and practices of financial institutions. Prior to proposing the regulation, the DFS surveyed almost 200 regulated banking and insurance institutions to identify best practices and emerging risks. The DFS has been particularly focused on risks posed by third-party service providers, as detailed in an April 2015 DFS report titled “Update on Cyber Security in Banking Sector: Third-Party Service Providers.”

The proposed regulation is subject to a 45-day notice and comment period prior to final issuance. More information is available here and a copy of the proposed language can be found here.

Categories

Cybersecurity, Privacy & Data Protection | Policy & Regulation | Compliance

London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.