New York Establishes New Cyber Security Examination Process for Financial Institutions

New York's Department of Financial Services released a letter on December 10, 2014, announcing the details of its plan to focus more attention on cyber security matters in conducting examinations. Directed at New York-chartered or -licensed banking institutions, the letter notes that the Department will be incorporating a number of new security-oriented questions and topics into its pre-examination "First Day Letters." Those questions and topics, outlined below, are similar to those in a more comprehensive cyber security questionnaire attached to a United States Securities and Exchange Commission's Office of Compliance Inspections and Examinations' ("OCIE") Risk Alert that was issued on April 15, 2014. The OCIE used its questionnaire earlier this year in conducting a limited set of cyber security examinations of registered investment advisors and broker-dealers. Together, both underscore the need for financial institutions to adopt and implement strong governance principles and controls to protect valuable information.

Under the examination process as announced by New York's Department of Financial Services, the Department will assess banks on their readiness to anticipate, respond to and combat cyber security threats in an effort to "encourage a laser-like focus on this issue by both banks and regulators," according to Benjamin M. Lawsky, Superintendent of the Department of Financial Services. In the letter, the Department identifies several topic areas on which its examinations will focus, including:

- Corporate governance and cyber security reporting structures;
- Resources devoted to information security and overall risk management;
- Protections against intrusion, including penetration testing, multi-factor or adaptive authentication and server and database configurations;
- Incident detection and response processes, including monitoring;
- Training of information security professionals as well as all other personnel; and
- Management of third-party service providers.

The Department expects to conduct cyber security examinations following an institution's comprehensive risk assessment.

The Department also released a list of direct questions to which it expects to seek responses as part of a cyber security risk assessment. Matters the questions touch on include:

- The qualifications of the institution's Chief Information Security Officer, or the individual otherwise responsible for information security;
- The extent to which the institution maintains information security policies and procedures;
- The institution's data classification approaches and data access management controls;
- The institution's vulnerability management programs, including its consideration of applications, servers, endpoints, mobile, network, and other devices;
- The institution's patch management program, including how updates, patches and fixes are obtained and disseminated;
- The institution's due diligence process regarding information security practices used to vet, select and monitor third-party service providers;
- Application development standards used by the institution, including the extent to which security and privacy requirements are incorporated into application development processes;
- The institution's incident response program, including how incidents are reported, escalated and remediated; and

- The relationship between information security and the organization's business continuity program.

The Department's letter is another sign of the increasing focus regulatory agencies are placing on the need for financial institutions to have adequate technical and administrative controls in place to protect sensitive data. In the face of these initiatives on cyber security, financial institutions should regularly review their existing policies, and conduct gap analyses against regulatory and market expectations to ensure their data governance practices adequately address continuously evolving cyber threats. There are a number of tools financial institutions can use in conducting such analyses, including the "Framework for Improving Critical Infrastructure Cybersecurity" released by the National Institute of Standards and Technology.

For more information about how to prepare your organization to respond to cyber security assessments by regulators or how to otherwise handle cyber security-related compliance matters, please contact a member of Ropes & Gray's leading privacy & data security team, such as Jim DeGraw, Seth Harrington, David McIntosh, Doug Meal, Elizabeth Reza, Mark Szpak or Michelle Visser, or your regular Ropes & Gray contact.

James S. DeGraw
Seth C. Harrington
David McIntosh
Douglas H. Meal
Elizabeth J. Reza
Mark P. Szpak
Michelle Visser