Cullen | Dykman

New York State Department of Financial Services Issues Expanded Cyber Security

December 12, 2014

As part of an ongoing effort to combat cyber attacks on financial institutions and promote enhanced cybersecurity, the New York State Department of Financial Services ("DFS") has issued expanded examination procedures focusing specifically on cybersecurity and information technology ("IT") issues. The expanded examination procedures were issued on December 10, 2014, and are applicable to all New York State-chartered banks.

The expanded cybersecurity examination procedures will be integrated into DFS's regular examination process going forward and implemented through updated pre-examination "First Day Letters" and revised procedures for scheduling and assessing IT/cybersecurity examinations.

The updated "First Day Letter" of IT/cybersecurity examinations will now include, but not be limited to, the following topics: IT management and corporate governance for cybersecurity-related issues, risk assessment and management, network security such as multi-factor authentication, information security testing and monitoring, incident detection and response, training, vendor management, business continuity and disaster recovery plans, and cybersecurity insurance coverage.

Additionally, the timing for IT/cyber security examinations has been adjusted. Such examinations will now be scheduled after the comprehensive risk assessment of each institution. During risk assessments, banks will be asked by the DFS for responses to the following items:

- Provide the CV and job description of the current Chief Information Security Officer or the person responsible for information security, detailing that individual's information security training, experience, and related reporting lines. In addition, provide an organization chart for the IT and information security functions.
- Describe the information security policies and procedures addressing confidentiality, integrity, and availability, and provide copies of all such information security policies.
- Describe the integration of data classification into information risk management policies and procedures.
- Describe the bank's vulnerability management program for servers, endpoints, mobile devices, network devices, systems, and applications.
- Describe the bank's patch management program including how updates, patches, and fixes are obtained and disseminated, whether processes are manual or automated, and how often they occur.
- Describe identity and access management systems for both internal and external users.

- Identify and describe the current use of multi-factor authentication for any systems or applications.
- Describe the due diligence process regarding information security practices that is used in the vendor management process.
- Describe all application development standards used, such as the use of a secure software development life cycle.
- Provide a copy of, or describe, the bank's incident response program detailing how incidents are reported, escalated and remediated.
- Describe the extent to which information security is incorporated into the bank's business continuity/disaster recovery plan, and this plan's testing frequency and results.
- Describe any significant changes to the IT portfolio over the past 24 months resulting from mergers, acquisitions, or new business lines.

If you have any questions regarding the new guidance or cybersecurity issues in general, please feel free to contact Joseph D. Simon at 516-357-3710 or via email at jsimon@cullenanddykman.com, Kevin Patterson at 516-296-9196 or via email at kpatterson@cullenanddykman.com, or Mandy Xu at 516-357-3850 or via email at mxu@cullenanddykman.com.

Practices

- Banking and Financial Services
- Regulatory and Compliance
- Corporate
- Cybersecurity and Data Privacy

Industries

- Financial Institutions
- Insurance

Attorneys

- Kevin Patterson
- Joseph D. Simon