Cooley

New Cybersecurity Rules for Financial Institutions

October 11, 2016

Last month, both Federal and state regulators affirmed their commitment to preventing and managing cybersecurity risk, particularly in the financial industry. First, the Commodity Futures Trading Commission (CFTC) **adopted** final rules on cybersecurity testing for certain US financial organizations. Second, Governor Andrew M. Cuomo of New York **announced** a "first-in-the-nation" cybersecurity regulation, which is focused on protecting consumers and financial institutions.

These announcements reflect a growing awareness of cybersecurity vulnerabilities, the exploits of which are increasingly sophisticated and difficult to detect. Both regulations also specifically affect New York, one of the world's financial centers. As a result, financial organizations in New York may, depending on their cybersecurity strategy, need to devote significant resources towards addressing and minimizing this emergent risk.

CFTC's Final Rules

On September 8, the CFTC adopted Final Rules on cybersecurity testing, applicable to derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories. The CFTC's rules require five types of security testing: (1) vulnerability testing; (2) penetration testing; (3) controls testing; (4) security incident response plan testing; and (5) enterprise technology risk assessment. In addition, the Final Rules require a minimum frequency of testing, use of independent contractors, and internal reporting and review procedures, including reports to senior management and boards of directors. The Final Rules also emphasize cybersecurity testing through ongoing risk assessments and board oversight. The scope and frequency of the cybersecurity testing depends on the type of financial organization.

The Final Rules reflect a heightened awareness of the vulnerabilities that companies, especially those in the financial sector, face when it comes to cybersecurity. Further, they demonstrate the importance of a flexible, risk-based approach to cybersecurity that can be adapted based on the type of organization and the specific threats that the organization faces.

New York's Proposed Cybersecurity Regulation

On September 13, Governor Andrew M. Cuomo announced a first-in-the-nation cybersecurity regulation that would require banks, insurance companies, and other financial services institutions regulated by the New York State Department of Financial Services to implement cybersecurity programs. The proposed regulation requires financial institutions to implement a cybersecurity program and a written cybersecurity policy, and designate a Chief Information Security Officer (CISO) responsible for overseeing and enforcing the program and policy. Importantly, Governor Cuomo's proposed regulation also requires financial institutions to have policies and procedures in place for ensuring the confidentiality of nonpublic data held by third parties. Governor Cuomo's proposed regulation is subject to a 45-day notice and comment period from its September 28 publication in the New York State register.

Like the CFTC's Final Rules, Governor Cuomo's proposed cybersecurity legislation requires minimum standards of security, but allows for flexibility so that the various financial organizations can keep pace with technological innovations and the changing environment around cyberattacks.

Implications

Both the CFTC's Final Rules and Governor Cuomo's proposed cybersecurity legislation are consistent with the increased regulatory focus on cybersecurity. For example, both the FTC and FCC have issued guidance on the importance of protecting against cyberattacks, which we covered on **September 22, 2016** and **October 6, 2016**. These announcements also reflect an awareness of the threat of cyberattacks in the financial industry, where cyberattacks are particularly prevalent. As a result, financial organizations must continuously monitor their systems for vulnerabilities and understand the types of cybersecurity threats they face with respect to their data. Ensuring accountability across the organization and at the level of senior management and boards of directors is also important. Cybersecurity is thus a critical component of any organization's corporate governance and approach to operational risk management. Complying with the CFTC's Final Rules (and, if passed, the proposed New York cybersecurity legislation) can pose complicated problems for companies that have to balance cybersecurity compliance with operational realities. Careful attention will be needed involving a variety of technical, physical, and operational requirements. Cooley lawyers are experienced in helping clients navigate these tricky waters.

Key Contacts

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090
