PUBLICATION

Looking Forward to 2017: Cybersecurity and the SEC

November 01, 2016

Fall is upon us and, even in an election year, it's not too early to begin thinking about the Securities and Exchange Commission's enforcement priorities for 2017. Regarding data protection, we predict that the SEC will continue to focus on cybersecurity and may even mandate that financial firms share information regarding cyber threats to maintain industry awareness of the risks to consumer information.

Why? Information sharing is now hitting its stride as a countermeasure in the cybersecurity world. In late 2015, the Cybersecurity Information Sharing Act (CISA) became law. CISA was designed by Congress to "improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes." The law, among other things, allows the U.S. government and private entities to share "cyber threat indicator" information. CISA even provides private entities immunity from suit for such sharing.

At the same time, the need to improve cybersecurity in the financial arena has not been lost on the Executive Branch. For three years in a row, the SEC has named cybersecurity a top concern, especially in connection to internal security program assessment and evaluation. This year, for example, the Office of Compliance Inspections and Examinations (OCIE) has focused on cybersecurity protocols implemented by financial firms to protect consumer information from cyberattacks. As investment advisors and broker dealers well know, OCIE examiners ask hard questions about the effectiveness of protective procedures, and the SEC expects written policies, procedures and training to ensure security measures are implemented, systematically followed and effective.

The year before this followed the same pattern. The SEC's 2015 cybersecurity initiative also focused on the protection of consumer information collected, held and used by investment firms. This emphasis resulted from the increased use of diverse technology by advisors and dealers in business transactions that require the exchange of sensitive financial information. Added to that, repeated and high-profile data breaches undermined consumer confidence, resulting in a need for stricter standards for protecting confidential data. Thus, for example, funds and advisors are now required to test security systems and evaluate the effectiveness of internal practices.

None of this came as a surprise, of course, as the SEC had issued detailed guidance back in 2011 regarding disclosure obligations relating to cybersecurity risks and cyber incidents. But, the SEC's sustained focus on cybersecurity over the last few years underscores the real need to identify risks, build an effective security framework, monitor the program and establish procedures for responding to cyberattacks. Proof that safeguards for personal and sensitive information are adequate is not optional. Periodic risk assessments and documented benchmarks for success are an unavoidable part of verifying compliance with SEC obligations. Further, ongoing investigations to determine internal and external cybersecurity threats and vulnerabilities are necessary to avoid noncompliance and to ensure new information about cyberattacks is incorporated appropriately into existing security programs.

In short, while we lack a crystal ball, we think cybersecurity information sharing and the SEC's 2017 priorities will begin to converge in 2017, bringing a new urgency to the need for clients to strengthen protections for customer data. Stay tuned…