CARLTON FIELDS

SEC Commissioner Encourages Commission to Bolster its Own Cybersecurity

CYBERSECURITY AND PRIVACY | SECURITIES AND DERIVATIVE LITIGATION | SECURITIES TRANSACTIONS AND COMPLIANCE | DECEMBER 17, 2015

On December 16, SEC Commissioner Luis Aguilar issued a statement regarding the SEC's cybersecurity protocols for its data gathering efforts. Commissioner Aguilar's statement follows various SEC initiatives to gather information about the securities markets that have led some market participants to worry about the strength of the SEC's cybersecurity. In his statement, Commissioner Aguilar addressed current SEC cybersecurity measures and made recommendations he believes would allow the SEC to shore up its role as steward of sensitive personal and financial data.

In his statement, Commissioner Aguilar observed that "the most useful tool any regulator can possess is accurate and complete information on which to base its decisions." Gathering this data has become increasingly difficult as the network of trading venues has increased to include 11 exchanges, approximately 44 alternative trading systems, and more than 200 broker-dealers. Monitoring these venues requires the SEC to access and safeguard vast amounts of information, information that is constantly at risk of a data breach.

Acknowledging the SEC's data modernization efforts, Commissioner Aguilar notes the various ways in which the SEC has revolutionized data including the planned Consolidated Audit Trail (CAT), which will allow the Commission to track trading activity for all major stocks in the United States; and the Division of Economic and Risk Analysis's Quantitative Research Analytical Data Support program, which generates standardized quantitative reports of financial markets and registrant activities. Commissioner Aguilar cautioned that while the data marshalled by these efforts is invaluable to the SEC, it is also invaluable to cyber criminals.

Concerns about the SEC's insufficient cybersecurity measures partly stem from reports from the Governmental Accounting Office (GAO) and the Inspector General. The GAO's April 2015 report found that the SEC has "not consistently implement[ed] effective internal controls over its informational systems operations," and found weaknesses relating to "baseline standards" and "security configurations" for "password settings and network services." The Inspector General's February 2015 report similarly noted several specific weaknesses, including a "lack of full implementation of continuous monitoring" and "outdated procedures and inconsistences with policies."

Remedying these concerns requires a multi-pronged attack, according to Commissioner Aguilar, with efforts including training personnel to help them recognize and manage key cybersecurity threats, monitoring and updating policies and processes, focusing on internal defenses in addition to perimeter defenses, and insuring that third-party software developers incorporate sufficient security at the outset into products they sell to the SEC.