Insights for All Companies from the SEC's Cybersecurity Examination of Regulated Financial Entities

By Sabastian V. Niles and Marshall L. Miller

In August 2017, the Office of Compliance Inspections and Examinations ("OCIE") of the Securities and Exchange Commission released the results of its second Cybersecurity Initiative, which examined cybersecurity-related preparedness and implementation efforts by 75 regulated financial entities. The resulting OCIE Risk Alert depicts an industry demonstrating heightened sensitivity to cyber risks, but also experiencing gaps between policy ambition and day-to-day execution, and confronting growing pains associated with accelerated change, including the introduction of significant new policies and procedures that may lack focus or consistent implementation. While the Risk Alert directly addresses the cybersecurity procedures of broker-dealers, investment advisers, and other SEC-regulated entities, companies in all industries should consider assessing their practices with respect to the issues highlighted by the SEC.

Overall, the SEC reported improvement in preparedness since its first Cybersecurity Initiative in 2015. According to OCIE staff, nearly all of the companies examined now maintain the basic building blocks for a sound cybersecurity program, including written cybersecurity policies and procedures, periodic system and vendor risk assessments, regular system maintenance, cyber incident response plans, and assignment of cybersecurity roles and responsibilities, whether or not a formal cybersecurity organizational chart is prepared. But the Risk Alert also stressed areas where planning was inconsistent, such as response plans addressing only a subset of potential incidents and failing to account for notifying impacted third parties, and highlighted instances where program implementation was found lacking, including inadequate installation of software patches and operating system upgrades, policies that provide

general guidance without articulating execution procedures or create "contradictory or confusing instructions for employees," and ambitious program requirements that are not fulfilled, such as "regular" testing not performed regularly, "mandatory" training not actually provided, and "high-risk" findings from vulnerability scans not timely remediated.

Based on its analysis of the industry's most robust programs, the SEC's OCIE staff recommended six elements for a successful cybersecurity program: (1) systems for maintaining inventories of data, information, and vendors; (2) detailed cybersecurity policies with a focus on execution; (3) data and system testing procedures with prescriptive schedules; (4) strong controls over data and system access; (5) mandatory training programs with procedures to ensure consistent implementation; and (6) engaged senior management.

The Risk Alert is a critical benchmark for SEC-regulated entities, but also a valuable tool for companies outside the financial industry. While cybersecurity programs should be tailored to particular company and industry risks, data sensitivities, and dynamics, taking into account the applicable regulatory environment and balancing ambition with practicalities, careful attention to the principles, pitfalls, and best practices identified by the SEC in its Risk Alert can help all companies navigate the ever-evolving cybersecurity landscape.

Sabastian V. Niles is a partner at Wachtell, Lipton, Rosen & Katz. **Marshall L. Miller** is of counsel in the Litigation Department at Wachtell, Lipton, Rosen & Katz.

Disclaimer

This entry was posted in Cybercrime & Cybersecurity, Financial Institutions, Governance, Risk management, Securities and Exchange Commission (SEC) and tagged Marshall L. Miller, Sabastian V. Niles on September 6, 2017 [https://wp.nyu.edu/compliance_enforcement/2017/09/06/insights-for-all-companies-from-the-secs-cybersecurity-examination-of-regulated-financial-entities/] by Michelle Louise Austin.