January 28, 2020

Insights for All Companies from the SEC-OCIE's Cybersecurity and Resiliency Observations

Yesterday, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") released a set of staff observations cataloguing OCIE's assessments of industry practices concerning cybersecurity and resiliency that are notable for their clarity and brevity. The observations address:

- governance and cybersecurity risk management,
- strategies concerning access rights and controls,
- data loss prevention measures,
- mobile devices and mobile application security considerations,
- incident response, business continuity, and resiliency,
- vendor management and third-party relationships,
- internal training and organizational awareness, and
- additional resources (e.g., information sharing groups).

OCIE has specially assessed information security for the past eight years, and through conducting compliance examinations of thousands of broker-dealers, investment advisers, clearing agencies, national exchanges, and other registrants annually, OCIE has deep insight into actual practices that have been implemented.

Although the exact contours of any corporate cybersecurity program should be tailored to each company's profile and operations, OCIE's statement highlights robust board and senior leader engagement in cybersecurity risk management and oversight as an indispensable component. Further, by linking cybersecurity and resilience planning, the OCIE statement underscores the need for companies to assess and consider the adequacy of post-incident response, recovery, and reporting plans alongside defensive mechanisms. OCIE's survey also highlights the intense regulatory focus, particularly in the financial services industry, on the necessity of an effective cybersecurity program.

As previously discussed, we continue to recommend that companies consider guidance issued by entities like OCIE as tools to develop their own benchmarks for oversight and design of effective enterprise-wide cybersecurity and resiliency programs.

Richard K. Kim
David B. Anders
Sabastian V. Niles
Jeohn Salone Favors