Kit Addleman, Tim Newman and Carrington Giammittorio on The American Bar Association Website: 'A Look at SEC's Last Decade of Cybersecurity Enforcement Efforts, Part II: Focus on Registered Entities'

February 17, 2022 Kit Addleman, Tim Newman, Carrington Giammittorio

PRACTICES Litigation, Corporate Governance, Crisis Management

A decade ago, the Securities and Exchange Commission (SEC) increased its focus on cybersecurity and the impact that cybersecurity incidents and risks have on the market and on investors. For public companies, the commission began to focus on what those companies were saying (or not saying) about cybersecurity incidents they suffered or the cybersecurity risks that affect their businesses. For regulated entities like registered investment advisors and broker-dealers, the commission's attention was heightened on cybersecurity controls— i.e., what policies and procedures did registered entities have in place to protect customer data and to prevent, detect, and respond to cybersecurity attacks?

Over the past 10 years, the commission has discussed cybersecurity obligations under federal securities laws through staff-level and commission-level guidance, comment letters, division priorities and alerts, a section 21(a) report of investigation, and, more recently, enforcement actions. This is the second article in a two-part series. In Part I, we discussed the SEC's focus on public company disclosure obligations. In this second article, we focus on the SEC's scrutiny of registered entities' cybersecurity controls.

Exam Priorities and Alerts

The SEC's Division of Examinations (formerly known as the Office of Compliance Inspections and Examinations, or OCIE) has explicitly included cybersecurity concerns in its examination priorities since 2012. Over that period, the division has published eight risk alerts touching on cybersecurity matters, steadily upping the ante on the topic.

The earliest risk alerts included cybersecurity matters almost as an aside. For example, a 2012 risk alert on social media use by investment advisors contained a single paragraph on information security, noting that "[a]lthough hacking and other breaches of information security can be posed in multiple ways, use of social media, especially third party social media sites, may pose elevated risks." Investment Adviser Use of Social Media (Jan. 4, 2012).

Excerpted from *The American Bar Association*. To read the full article, click here.