Six Quick Cybersecurity Takeaways from SEC Speaks 2021

October 18, 2021

On October 13, the annual Securities and Exchange Commission Speaks seminar concluded with presentations from the Examination, Enforcement, and Investment Management divisions. As SEC regulated entities (including publicly traded companies, investment advisers, and broker-dealers) look to 2022, they should keep the following key cybersecurity takeaways in mind:

- Continued Focus on Corporate Governance. The Associate Director of the Division of Examination's Technology Controls Program ("TCP") emphasized the continued importance of strong corporate governance relating to cyber, including cyber posture, senior leadership oversight of potential cybersecurity risk, and vendor risk management. In its action against First American, the SEC made clear that directors and officers play a critical role in developing a culture that values cyber hygiene, as well as setting up the reporting systems, testing, and training that allow important information regarding cyber threats to flow up to management. SEC registrants should continue to review how senior executive leadership and the board are involved in cybersecurity, and check for policies and systems that would facilitate leadership's timely engagement in critical cyber issues.

- Cyber Preparedness: TCP also specifically noted that exams will focus on four key cyber areas, among other topics: vendor management, company-wide cybersecurity risk management, operational resiliency, and incident response. Notably, these categories generally reflect the SEC's 2021 cybersecurity priorities.

- Holistic Policy Implementation: The Division of Enforcement reiterated that all registrants should not only adopt cybersecurity policies and procedures tailored to their business, but should also ensure that these are implemented across all systems where customer data is stored. The SEC has reminded registrants of this need multiple times (here, here, and here), suggesting that the SEC is becoming less tolerant of delinquent risk remediation going forward.

- Increased Outreach: Registrants should also expect outreach from the SEC during cybersecurity events to determine the scope and severity of the incident. This is novel but not surprising given the increasing frequency and severity of such incidents, particularly ransomware attacks at companies. Registrants should consider (a) revising their incident response plans to ensure that the internal stakeholders

who typically handle SEC communications are engaged; (b) drafting placeholder statements to the SEC in advance, so those statements can be adapted during an actual incident rather than being drafted from scratch at a time of crisis; and (c) incorporating SEC responses into tabletop exercises.

- Accurate, Succinct Disclosures: Companies should be careful about how they disclose the nature and extent of any cyber incident. As the SEC's August 2021 enforcement action against Pearson Plc reflects, the SEC will scrutinize potentially misleading statements that, for example, overstate the merits of a firm's cybersecurity program. Notably, the SEC plans to release Proposed Rules on Cybersecurity Disclosures in a matter of days, which should provide greater clarity in this area.

- Proactive Discussions on Tech Plans: Registrants should also take proactive steps to communicate with regulators regarding plans to adopt new technologies, such as blockchain, including with the Disclosure Review and Accounting Office to ensure they meet the substantive requirements.

* * *

Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Avi Gesser
agesser@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Charu Chandrasekhar
cchandra@debevoise.com

Matthew C. Rametta
mcrametta@debevoise.com

SAN FRANCISCO

H Jacqueline Brehmer
hjbrehmer@debevoise.com