BRACEWELL

INSIGHTS

Cyberattacked: The SEC Joins the Club

September 25, 2017

On September 20, the Securities and Exchange Commission announced that its system for electronic filing for public company disclosures, EDGAR, was compromised last year and that hackers may have used exposed information for illicit trading. The disclosure, which provided few details, offered the Commission the opportunity to issue a larger, wide-ranging statement describing its efforts to promote effective cybersecurity practices—inside the Commission itself as well as with respect to the market more broadly and the market participants it regulates. Notably, the statement highlights its continued, active investigation and enforcement of cybersecurity-related failures.

The *Statement on Cybersecurity*, released by Chairman Jay Clayton on September 20, 2017, did not indicate when the specific cyber-intrusion occurred but acknowledged that it resulted in access to nonpublic information:

> *In August 2017, the Commission learned that an incident previously detected in 2016 may have provided the basis for illicit gain through trading. Specifically, a software vulnerability in the test filing component of our EDGAR system, which was patched promptly after discovery, was exploited and resulted in access to nonpublic information. We believe the intrusion did not result in unauthorized access to personally identifiable information, jeopardize the operations of the Commission, or result in systemic risk. Our investigation of this matter is ongoing, however, and we are coordinating with appropriate authorities.*

The *Statement on Cybersecurity* is available in its entirety ***here***. It is unclear whether the 2016 incident occurred before or after a GAO review of the Commission's FY 2016 cybersecurity protocols that found that the agency had not fully implemented certain recommended intrusion detection capabilities. *See* GAO report, *SEC Improved Control of Financial Systems but Needs to Take Additional Actions* ***here***.

Instead of offering detail regarding the incident, the Statement sets forth the Commission's understanding of its role in promoting cybersecurity as "[d]ata collection, storage, analysis, availability and protection (including security, validation and recovery) have become fundamental to the function and performance of our capital markets, the individuals and entities that participate in those markets, and the U.S. Securities and Exchange Commission." The Statement broadly summarizes key areas of cybersecurity risk faced by both the Commission and its regulated entities:

I. Collection and Use of Data by the Commission

The Commission describes three main categories under which it receives, stores, and transmits data. First is the public-facing data that is submitted to and accessed through Commission

systems, most prominently, EDGAR. Over 50 million pages of disclosure documents are accessed on EDGAR daily and the system receives over 1.7 million electronic filings per year. Second, the agency handles data—including nonpublic information and personally identifiable information—in relation to its supervisory and enforcement functions. This data includes information obtained by staff in its Divisions of Investment Management and Enforcement and OCIE. Third is data that is maintained by the Commission relating to its internal operations, such as personnel records and internal controls records.

II. Management of Internal Cybersecurity Risks

The Statement describes how the Commission faces frequent attempts by unauthorized actors to access its systems in order to, among other things, reap illicit trading profits from nonpublic information, place fraudulent filings on the system, or disrupt public access to information. Also—like other agencies, financial market participants, and private sector entities—the Commission is at risk of unauthorized actions or disclosures by its own personnel as well as in connection with its third-party vendors. To combat these risks, the Commission has emphasized informed governance, policies and procedures, independent auditing, and external reporting to oversight agencies and committees.

Note that the Commission, as a federal agency, is subject to the May 11, 2017 ***Executive Order***, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which, among other things, requires a top-down cyber policy review of the government's systems, adopts the NIST Framework for Improving Critical Infrastructure Cybersecurity, and expresses preferences for uniformity and shared IT solutions across agencies. The Commission's vendors, like all government contractors, must stay abreast of the agency's implementation of these principles to ensure provision of services complies with any emerging regulations or policies.

III. Incorporation of Cybersecurity Considerations in the Commission's Disclosure-Based and Supervisory Efforts

The Commission outlines that its cybersecurity considerations cover three main areas. First, with respect to promoting effective public company disclosures, the Commission highlights the 2011 ***cybersecurity guidance*** issued by the Division of Corporate Finance, which provides principles that issuers should consider when addressing cyber risk in public disclosures. By citing this disclosure guidance and referring to disclosure-related enforcement activity in a later section, the Statement reflects recent comments by Chairman Clayton that public companies may not be providing enough information to investors regarding cybersecurity, *see* July 12, 2017 *Remarks at the Economic Club of New York* ***here***, and underscores the Commission's interest in this area.

Second, relating to oversight of market infrastructure, the Commission referenced Regulation SCI, which is designed to strengthen the technology infrastructure of securities markets, including exchanges and clearing agencies. Third, in terms of its role overseeing broker-dealers, investment advisers, and other market participants, the Statement discusses Regulation S-P (the Safeguards Rule); Regulation S-ID, addressing red flags for identity theft; and OCIE's emphasis on cybersecurity in its examination program.

See Bracewell commentary on SEC cybersecurity-related activities: *OCIE Releases Cybersecurity Risk Alert*, ***here***; *SEC Announces First Cybersecurity Enforcement Action Against an Investment Adviser for Failure to Protect Client Data*, ***here***; *SEC: 2015 Examination Priorities – Cybersecurity Compliance and Controls*, ***here***.

IV. Coordination With Other Governmental Entities

Not only does the Commission coordinate with other financial regulators like the Federal Reserve, the CFTC, the OCC, and the FDIC, it also collaborates with the FTC and the CFPB. Additionally, the Commission participates in interagency working groups, such as the Financial Stability Oversight Council and Financial and Banking Information Infrastructure Committee, and industry groups, such as the Financial Services Section Coordinating Council. The agency also seeks to coordinate with non-U.S. regulators.

V. Enforcement of the Federal Securities Laws

The Statement briefly mentions that enforcement actions can arise from a failure to address cybersecurity risks in public disclosures. While, to date, the Commission has not brought a single enforcement action relating to public disclosure of a cybersecurity incident or risk, the Commission's attention to this topic suggests that it is continuing to investigate and analyze cybersecurity incident and risk disclosures and could begin bringing such enforcement actions.

The Statement then turns to other examples of cybersecurity-related enforcement activities. Touting both the agency's innovative technology and analytical tools to detect suspicious market activity and the substantial expertise of the Division of Enforcement, the Statement references recent enforcement actions brought against hackers who sought to steal information relating to nonpublic merger negotiations and other hackers who accessed newswire services for nonpublic information relating to corporate earnings announcements. The Statement also refers to an action relating to a scheme to make unauthorized stock trades to drive up share prices and generate profits for other accounts.

VI. Looking Forward

In recognition of the vast amounts of sensitive data that it maintains, the Commission states its commitment to ongoing evaluation of when and how it collects such data, and how it can most effectively protect it while carrying out its mission. For example, in order to reduce the market sensitivity of some data, the Commission may collect it on a delayed basis.

Find additional Bracewell analysis relating to cybersecurity ***here***.