Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Expect More SEC Cybersecurity Enforcement This Year

By **Doug Davison, Adam Lurie and Meredith Riley** (January 17, 2019, 12:48 PM EST)

Doug Davison

Adam Lurie

Meredith Riley

The U.S. Securities and Exchange Commission has progressively turned its attention toward cybersecurity issues over the last several years, recently intensifying its focus and revamping its approach to regulation and enforcement throughout 2018. As a result, the SEC has become a key actor in protecting customers, markets, and investors from the evolving cybersecurity risks and abuses that have proven to be prevalent, serious, and potentially catastrophic.

The SEC is forcing U.S. market participants to address cybersecurity issues through its regulation of public companies and securities offerings, by both applying traditional tools of disclosure and enforcement to the cybersecurity arena and by expanding into the use of new or previously unused tools. Thus, parties involved in offering securities in the U.S. need to assess cyber-related disclosures to investors or face potential enforcement action for false or misleading statements in violation of the anti-fraud provisions of the federal securities laws. Moreover, companies with inadequate controls may find themselves not only to be victims of cyberattacks, but also subsequently under SEC investigation and subject to possible SEC action for not doing enough to prevent those attacks or failing to adequately respond to them when they happen. These efforts are likely to increase in 2019.

SEC Cybersecurity Initiatives Through 2018

The SEC's most recent focus on cybersecurity issues began in September of 2017, when it issued an eight-page statement disclosing that the Edgar system had been hacked the previous year and that illicit trading may have taken place based on the acquired information.[1] The statement also outlined both the steps the SEC would take internally to assess, implement and manage its own cybersecurity controls, and its approach to cybersecurity regulation of publicly traded companies and the securities market.[2] Only a few days later, the SEC announced the creation of a "Cyber Unit" within the Division of Enforcement that would consolidate the SEC's expertise in order to identify, investigate and address cybersecurity threats.[3] In launching the unit, Enforcement Division Co-Director Stephanie Avakian stated that "[c]yber-related threats and misconduct are among the greatest risks facing investors and the securities industry" and called cybersecurity "an area of critical national importance."[4]

February 2018 Interpretive Guidance on Public Company Cybersecurity

Disclosures

In February of 2018, the SEC issued interpretive guidance that specifically addressed cybersecurity disclosures, policies and procedures.[5] Expanding on previous 2011 guidance, it made clear that requirements for public company disclosures apply to cybersecurity matters, and that attention to those issues should be integrated into key disclosure areas such as risk factors, business description, legal proceedings, financial statements, board oversight, and company financial condition and results of operations.[6] It explained that the materiality of such information should be assessed using the same facts-and-circumstances analysis otherwise applicable in SEC disclosures — i.e., whether a reasonable investor would consider the information important in decision-making or would see it as significantly altering the total mix of available information.[7] The SEC also emphasized that companies should avoid generic boilerplate disclosure language and instead specifically tailor disclosures to their particular company and business model.[8] While it allowed that companies may need time to investigate an incident and cooperate with law enforcement, the SEC underscored that disclosure must still occur.[9]

The February 2018 guidance also addressed disclosure controls and procedures, requiring that such procedures be designed and implemented to ensure that cybersecurity information is elevated quickly, to allow for timely decision-making and disclosure.[10]

Major Enforcement Actions in 2018

Insider Trading (Equifax Inc.)

The SEC's February 2018 guidance also noted that information regarding cybersecurity breaches, vulnerabilities, and risks could be considered material nonpublic information and that insider trading policies should specifically address and seek to prevent trading on this information.[11] Underscoring that guidance, the SEC filed two separate enforcement actions against now former Equifax employees for trading on the basis of material nonpublic information regarding a data breach at the company that affected more than 140 million people. In one case, the SEC alleged that, after discovery of the breach but prior to its public disclosure, Equifax's chief information officer at the time, sold all of his nearly $1 million of vested stock to avoid losses of $117,000.[12] In the other case, the SEC alleged that a software developer who was in charge of creating a website for affected customers surmised that the breach victim was Equifax itself and subsequently earned $75,000 through bets placed in the put options market.[13]

Failure to Disclose Cybersecurity Incidents (Yahoo Inc.)

The SEC continued to highlight the importance of its February 2018 guidance through major enforcement actions in 2018. In May, it imposed a $35 million penalty on Yahoo successor entity Altaba, concluding the first-ever cybersecurity enforcement action against a public company for the consequences of failing to timely disclose a data breach.[14] Yahoo had been breached in 2014, when hackers associated with the Russian Federation stole personal information for hundreds of millions of the company's users.[15] While the breach was quickly reported to the company's senior management and in-house counsel, the SEC alleged that it was never investigated, reported to auditors or outside counsel, or disclosed to investors.[16] Yahoo subsequently made numerous annual and quarterly reports that failed to disclose the breach.

Ultimately, it was not revealed until its 2016 acquisition by Verizon Communications Inc.[17] The SEC found that Yahoo violated Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933, for failure to disclose material information, and Section 13(a) of the Securities Exchange Act of 1934 and Rules 12b-20, 13a-1, 13a-11, 13a-13, and 13a-15, for failures in disclosure controls and procedures.[18] SEC Enforcement Division Co-Director Steven Peikin called Yahoo's response to the breach a "complete corporate failure" and stated that the enforcement action and penalty "should serve as a message to other companies."[19]

Identity Theft Red Flags Rule (Voya Financial Advisers Inc.)

The SEC concluded another first-of-its-kind enforcement action in September of 2018, for violations of Regulation S-P, 17 C.F.R. 30(a) (the Safeguards Rule) and the previously unenforced Identity Theft Red Flags Rule (Rule 201 of Regulation S-ID). This rule requires investment firms to create and maintain a policy that safeguards customer information from identity theft, and pay attention to "red flag" warning signs that hackers may be attempting to steal information. In 2016, hackers infiltrated Voya Financial Advisers and gained access to personal information for 5,600 VFA customers by calling a support hotline and requesting password resets.[20] Key to the SEC action was that VFA's policy had not been updated since being instituted a decade earlier, and that it was not administered by the company's senior management (as required by the rule).[21] In settling the SEC's charges, VFA agreed to pay a $1 million penalty, and was required to undertake a list of remedial actions and engage an independent compliance monitor.[22]

Investigative Report on Business Email Compromises

The SEC also issued an investigative report detailing business email compromises via cyber scams at nine public companies and whether those companies' failure to maintain cybersecurity related accounting control failures violated 13(b)(2)(B) of the Exchange Act, which requires accounting controls that ensure accordance with management authorization for the execution of transactions and access to assets within a company.[23]

The investigated companies fell prey to two types of schemes. In the first, perpetrators used a spoofed email domain to impersonate a senior company executive and induce an employee to make a large wire transfer. In the second, perpetrators impersonated a vendor or supplier by hacking into the email account of a legitimate employee. They would then redirect a wire transfer for an invoice to an account under the impersonator's control. Although these were relatively unsophisticated scams, the companies lost large amounts of often unrecovered funds, ranging from $1 million to over $45 million.[24] Although the SEC declined to bring action against the companies, it issued a report for the stated purpose of making other companies aware of both the existence of the schemes and the need to implement and adhere to internal accounting controls that address them.[25]

What to Expect in 2019

Continued Attention to Cybersecurity

This focus on cybersecurity will continue into and intensify throughout 2019, as illustrated in at least two end-of-year statements from the SEC. The Enforcement Division's 2018 annual report prominently highlighted its cybersecurity efforts. Cybersecurity, along with regulation of initial coin offerings and digital currency, is the backbone of one of the division's five principles of enforcement: "Keep Pace with Technological Change."[26] The report discussed the numerous cyber-related enforcement actions and detailed the SEC's impact on the intersection of securities laws and cybersecurity issues, noting that the SEC brought 20 cases in 2018 and had more than 225 ongoing investigations.

SEC Chairman Jay Clayton also devoted a significant portion of his recent congressional testimony to the SEC's cybersecurity enforcement efforts, stating that the resources devoted over the past year illustrate "the high priority that we continue to place on cyber-related issues affecting investors and our markets."[27]

Cybersecurity Areas of Focus

Companies should be aware of at least four likely areas of SEC activity this year:

Data Security Policies

The SEC has made clear that it expects companies to integrate cybersecurity concerns into their internal policies and procedures, particularly those related to data security. These policies need to be calibrated to the nature of the company's business and risks, and regularly updated for changing technologies and circumstances. Importantly, training about and compliance with these policies should be integrated throughout all levels of the organization. Cyberattack victims with inadequate data security policies will find themselves subject to enforcement action. The SEC is also likely to continue the use of third-party compliance monitors post-settlement.

Internal Accounting Controls

The SEC's October report on cyber scams was a clear indication that enforcement actions in this area are on the horizon. Although no action was taken against the nine investigated companies, the report's emphasis on 13(b)(2)(B) compliance was a warning that internal accounting controls must be adjusted to fit a business's cyber-related risks, and, in particular, able to withstand a communications environment rife with cyber fraud.

Public Company Reporting Disclosures

The SEC has also made clear that it considers certain cybersecurity issues to be within the scope of material information that must be disclosed to the public and investors. This is particularly the case with cybersecurity breach information, as illustrated by the Yahoo action, but also extends to the range of disclosures required in public company reporting. The SEC will be on the lookout for generic boilerplate language, and may insist on disclosures tailored to an industry and company.

Insider Trading Policies

The SEC has stated, and illustrated through its Equifax enforcement actions, that inside information about cybersecurity matters will be treated like other types of material nonpublic information. The SEC will be looking to see this explicitly reflected in a company's insider trading policies. It is likely to monitor for inside trading in this area, particularly between discovery of a breach and disclosure to the public, and will pursue enforcement actions as necessary.

Conclusion

The SEC's attention to cybersecurity issues is likely to increase in 2019, as it further adapts its traditional enforcement tools to the ever-changing area of cybersecurity, and continues to develop the infrastructure, resources and expertise required to meet the challenges that cybersecurity concerns present to U.S. market participants.

Doug Davison is a partner at Linklaters LLP and former counsel to former SEC Chairman Arthur Levitt.

Adam Lurie is a partner at the firm and head of the U.S. dispute resolution practice.

Meredith Riley is an associate at the firm.

[1] Public Statement, SEC, Statement on Cybersecurity (Sept. 20, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.

Hereinafter, "September 2017 Statement."

[2] September 2017 Statement.

[3] Press Release, SEC, SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors (Sept. 25, 2017), https://www.sec.gov/news/press-release/2017-176. Hereinafter, "Cyber Unit Statement."

[4] Cyber Unit Statement.

[5] Press Release, SEC, SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), https://www.sec.gov/news/press-release/2018-22; Public Statement, SEC, Statement on Cybersecurity Interpretive Guidance (Feb. 21, 2018), https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21; and Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 CFR 229 and 249 (Feb. 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf. Hereinafter, "February 2018 Guidance."

[6] February 2018 Guidance.

[7] February 2018 Guidance.

[8] February 2018 Guidance.

[9] February 2018 Guidance.

[10] February 2018 Guidance.

[11] February 2018 Guidance.

[12] Press Release, SEC, Former Equifax Executive Charged With Insider Trading (Mar. 14, 2018), https://www.sec.gov/news/press-release/2018-40.

[13] Press Release, SEC, Former Equifax Manager Charged With Insider Trading (June 28, 2018), https://www.sec.gov/news/press-release/2018-115.

[14] Press Release, SEC, Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million (Apr. 24, 2018), https://www.sec.gov/news/press-release/2018-71 and Altaba Inc., Securities Act Release No. 10485, Exchange Act Release No. 83096 (Apr. 24, 2018), https://www.sec.gov/litigation/admin/2018/33-10485.pdf. (Hereinafter, Yahoo! Press Release and Order.)

[15] Yahoo! Press Release and Order.

[16] Yahoo! Press Release and Order.

[17] Yahoo! Press Release and Order.

[18] Yahoo! Press Release and Order.

[19] Renae Merle, Yahoo Fined $35 Million for Failing to Disclose Cyber Breach, Wash. Post, Apr. 24, 2018, https://www.washingtonpost.com/news/business/wp/2018/04/24/yahoo-fined-35-million-for-failing-to-disclose-cyber-breach/?utm_term=.3425297df198.

[20] Press Release, SEC, SEC Charges Firm With Deficient Cybersecurity Procedures (Sept. 26, 2018), https://www.sec.gov/news/press-release/2018-213 and Voya Financial Advisors, Inc., Exchange Act Release No. 84,288 (Sept. 26, 2018),

https://www.sec.gov/litigation/admin/2018/34-84288.pdf. Hereinafter, "VFA Press Release and Order."

[21] VFA Press Release and Order.

[22] VFA Press Release and Order.

[23] Press Release, SEC, SEC Investigative Report: Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls (Oct. 16, 2018), https://www.sec.gov/news/press-release/2018-236; Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements, Exchange Act Release No. 84,429 (Oct. 16, 2018), https://www.sec.gov/litigation/investreport/34-84429.pdf. Hereinafter, "Cyber-scam Press Release and Order." See also Linklaters, U.S. SEC Warns Public Companies to Reassess Internal Accounting Controls in Light of Cyber Scams (Oct. 17, 2018), https://www.linklaters.com/en-us/insights/publications/us-publications/2018/october/us-sec-warns-public-companies-to-reassess-internal-accounting-controls-in-light-of-cyber-scams.

[24] Cyber-scam Press Release and Order.

[25] Cyber-scam Press Release and Order.

[26] Press Release, SEC, SEC Enforcement Division Issues Report on FY 2018 Results (Nov. 2, 2018), https://www.sec.gov/news/press-release/2018-250; Report, SEC, Annual Report, Division of Enforcement (Nov. 2, 2018), https://www.sec.gov/files/enforcement-annual-report-2018.pdf (hereinafter, "2018 Report").

[27] Oversight of the U.S. Securities and Exchange Commission: Hearing Before the S. Comm. On Banking, Housing, and Urb. Aff. (2018) (statement of Jay Clayton, Chairman, SEC) https://www.sec.gov/news/testimony/testimony-oversight-us-securities-and-exchange-commission-0.