New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 267—NO. 43

MONDAY, MARCH 7, 2022

When Security Fails: Increasing Focus at the SEC On Cybersecurity **Disclosure and Internal Controls**

BY DAVID R. OWEN, KENNETH RITZ AND ALEXA MOSES

Virtually all of the world's commercial data and information has become remotely accessible from almost anywhere, creating an explosion of corporate productivity and efficiency, as well as a never-ending stream of hackers hoping to take criminal advantage of it.

Virtually all of the world's commercial data and information has become remotely accessible from almost anywhere, creating an explosion of corporate productivity and efficiency, as well as a never-ending stream of hackers hoping to take criminal advantage of it. Recent COVID-19 lockdowns and mass migration to remote work have highlighted both the power and the continuing vulnerabilities of this evolution. To assist investors in understanding the evolving risks, the Securities and Exchange Commission (SEC) has shown a steadily increasing focus on cybersecurity disclosures in recent years, and that trend is almost certain to continue with new rule amendments expected in April of this year.

In a keynote speech on January 24, SEC Chair Gary Gensler said: "Cyber incidents, unfortunately, happen a lot. History and any study of human nature tells us they're going to continue to happen … . Given this, and the evolving cybersecurity risk landscape, we at the SEC are working to improve the overall cybersecurity posture and the resiliency of the financial sector." A key focus for Chair Gensler is the need to develop more uniform disclosures, observing that "companies and investors alike would benefit if [cyber risk disclosures] were presented in a consistent, comparable, and decision-useful manner."

As discussed further below, although the triggering event leading to SEC enforcement in most cases is a significant hacking or data breach incident, recent SEC press releases and orders indicate a high likelihood that when such events occur, the SEC now will undertake to review both the reasonableness of the security program and statements that preceded the incident, and any statements made about the incident itself, or the potential consequences going forward. Chair Gensler's statements echo several recent SEC orders that have aggressively charged companies for deficient cybersecurity disclosures, in addition to a lack of adequate internal reporting controls between the information security team and the executives responsible for disclosures. In this new environment, even "low-tech" issuers

Photo: Diego M. Radzinschi/ALM

Headquarters of the U.S. Securities and Exchange Commission in Washington, D.C.

DAVID R. OWEN *is a partner in Cahill Gordon & Reindel's New York office, advising leading financial institutions and global corporations in connection with data privacy and cybersecurity matters.* KENNETH RITZ *and* ALEXA MOSES *are associates at the firm.*

accordingly should take great care to review and align both their security program and any incident response so that all disclosures are fair and complete.

The Regulatory Framework

The existing regulatory framework for cybersecurity disclosures and related controls stems originally from 2011 guidance from the staff of SEC's Division of Corporation Finance, which did not explicitly require any disclosure at all, explaining that "no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents," and also that "companies nonetheless may be obligated to disclose such risks and incidents." The 2011 guidance further explained that "material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading." The staff identified specific areas to consider, including risk factors and disclosure controls. The guidance led many public companies to report their notable cybersecurity risks and incidents in regular SEC reporting.

In 2018, the SEC updated and expanded the 2011 guidance, highlighting a number of new principles to be applied, including the disclosure of any cyber risks and incidents in registration statements along with in Annual Reports on Form 10-K and Quarterly Reports on Form 10-Q, as "necessary to make the statements therein not misleading." The new interpretation also encouraged, but did not require, interim updates by way of a Current Report on Form 8-K or a Report of Foreign Private Issuers on Form 6-K "with respect to the costs and other consequences of material cybersecurity incidents." Notably, the 2018 interpretation did not create a requirement to disclose all cybersecurity-related incidents in filings, but it did provide a set of factors to consider when determining materiality of an incident or risk, including: (1) nature, extent and potential magnitude, (2) potential harm, including to company reputation, financial performance, and customer and vendor relationships, and (3) possibility of litigation or regulatory investigations. Pursuant to Rules 13-a15 and 15d-15 under the Securities Exchange Act of 1934 (the Exchange Act), the interpretation indicated that public companies should have policies and procedures in place to ensure that relevant information pertaining to cybersecurity risks and incidents is escalated promptly enough to allow "senior management to make disclosure decisions and certifications."

The 2018 interpretation stressed that a company must not only have the appropriate disclosure controls and procedures in place, but also must ensure timely collection and evaluation by appropriate personnel of information potentially subject to required disclosure, or relevant to an assessment of the need to disclose. According to the interpretation, "The [SEC] believes that the development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that a company has faced or is likely to face."

The Division of Corporation Finance is expected to propose that the SEC update its rules regarding cybersecurity disclosures in April 2022. Although the specifics are yet to be seen, it is expected to include more expansive disclosure obligations and an effort to make the language, standards and criteria applied more uniform across issuers. In fact, on Feb. 9, 2022, an SEC press release announced proposed rules regarding cybersecurity risk management for registered investment advisors and investment companies and business development companies, reinforcing that the SEC is heavily focused on cybersecurity practices and disclosures, including that the new rules would require reporting "significant" cybersecurity incidents to the SEC as well as in brochures and registration statements. Updated rules for determining materiality and the timeliness of disclosures also seem likely. With respect to disclosure controls specifically, it seems that the SEC also may require internal cybersecurity policies and procedures, and communication of relevant cybersecurity information and data breaches between the cybersecurity team and leadership responsible for making cybersecurity disclosure decisions.

Recent Enforcement Actions For Inadequate Controls

In almost all cases, it is the occurrence of a cyber-incident that attracts SEC enforcement attention, rather than

a generalized inadequacy of security controls or disclosure. Several recent SEC orders make clear, however, that the occurrence of a cyber-incident likely will lead to an expansive review and scrutiny of both the disclosures made about the incident, in addition to all prior security-related disclosures and the relevant controls that were in place to support them. Furthermore, the scope of recent SEC inquiries shows that it now expects a robust communication between the technical staff and the reporting executives to ensure that all disclosures are complete and do not omit important information.

On June 15, 2021, the SEC announced the settlement of charges against real estate settlement company First American Financial Corporation, a real estate settlement services provider, stemming from disclosures in its May 2019 press release and 8-K. Those statements had purported to disclose a sharing vulnerability that had inadvertently exposed over 800 million images containing social security numbers and financial information dating back to 2003. Although company disclosures had indicated a tip from a journalist on May 24, 2019 as the triggering event, the SEC order observed that security staff had in fact identified the vulnerability several months earlier, and that the company had failed to remediate it pursuant to company policy. Although the company stated that the senior executives responsible for public statements were never apprised of the discovery, the SEC was evidently unpersuaded that this should relieve the company of responsibility to include this information in the disclosure. As a result, the SEC deemed both the disclosure and the controls deficient, and the company was required to pay nearly half a million dollars to settle the issue.

On Aug. 16, 2021, the SEC settled charges against Pearson plc, a software provider to schools and universities, stemming from Pearson's disclosures in its July 2019 media statement and 6-K Risk Factors. Pearson's 6-K had referred to a data breach risk as "hypothetical" even after an actual breach affecting millions of students' records, and stated that the disclosure of the incident was only precipitated by media reports, rather than the internal discovery of the event by the company that had occurred earlier. The company poorly described the intrusion as an "authorized access" and speculated about the scope of the number of records and data covered and potential for misuse, when much more concrete information was already available to them. Notably, the SEC also faulted the disclosure of the security program in place as inadequate, citing a patching issue and failure to attend to the vulnerability that had triggered the data breach. The order specifically found that Pearson's controls were not reasonable either to assess or elevate the issue for disclosure, even though Pearson had created an incident management response team and retained third-party consultants to investigate the breach. In its order, the SEC charged Pearson with violations of Rules 17(a)(2) and 17(a)(3) of the Securities Act of 1933 and various other rules under the Exchange Act for the misleading statements, together with insufficient disclosure controls, and Pearson ultimately agreed to a $1 million penalty.

> To assist investors in understanding the evolving risks, the Securities and Exchange Commission (SEC) has shown a **steadily increasing focus on cybersecurity disclosures** in recent years, and that trend is almost certain to continue with **new rule amendments expected in April of this year.**

A retrospective scrutiny of internal controls in these recent cases is generally consistent with the SEC's public posture, and they show a willingness to scrutinize and charge conduct and disclosures that might previously have been deemed adequate if made in good faith. As recently as 2017, the SEC was telling issuers with respect to cyber incidents and risks, "We recognize this is a complex area subject to significant judgment, and we are not looking to second-guess reasonable, good faith disclosure decisions." How much of that statement remains accurate today is an open question in the current environment, and issuers should plan in advance for an inquiry into any material judgment calls, and implement a security program and response plan that can be defended in the event of a major incident.