October 3, 2017

Making Sense of the SEC Data Breach

by Scott Kimpel

Published in Law360

On Wednesday, Sept. 20, 2017, Jay Clayton, chairman of the U.S. Securities and Exchange Commission, made the surprising announcement that the SEC's EDGAR database — the agency's online document repository for periodic reports and registration statements filed by public companies and mutual funds — had been hacked:

> 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.[1]

Published after working hours with the key hacking revelation buried in dense text about unrelated cybersecurity initiatives at the SEC, the statement contains a paucity of details. In a subsequent press release, Clayton walked back the idea that no personally identifiable information had been compromised, revealing that names, dates of birth, and social security numbers of two individuals were accessed.[2] The original SEC statement also came on the heels of a July 2017 report by the Government Accountability Office that found the SEC had not fully implemented 11 previous GAO information security recommendations, including protecting SEC network boundaries from possible intrusions, identifying and authenticating users, authorizing access to resources, auditing and monitoring actions taken on SEC systems and network, and encrypting sensitive information while in transmission.[3] The GAO report also identified an astounding 26 information security deficiencies that remained unresolved as of September 2016.

Already scheduled to testify at an oversight hearing before the Senate Banking Committee on Sept. 26, Clayton provided additional color on the incident in prepared testimony:

> In August 2017, in connection with an ongoing investigation by our Division of Enforcement, I was notified of a possible intrusion into our EDGAR system. In response to this information, I immediately commenced an internal review. Through this review and the ongoing enforcement investigation, I was informed that the 2016 intrusion into the test filing component of our EDGAR system provided access to nonpublic EDGAR filing information and may have provided a basis for illicit gain through trading.

> We believe the 2016 intrusion involved the exploitation of a defect in custom software in the EDGAR system. When it was originally discovered, the SEC Office of Information Technology (OIT) staff took steps to remediate the defect in custom software code and reported the incident to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT). Based on the investigation to date, OIT staff believes that the prior remediation effort was successful. We also believe that the intrusion did not result in unauthorized access to personally identifiable information, jeopardize the operations of the Commission or result in systemic risk. Our review and investigation of these matters, however, as well as the extent and impact of the intrusion and related illicit activity, is ongoing and may take substantial time to complete.[4]

Perhaps coincidentally, the SEC's inspector general released a heavily redacted audit report on Sept. 29, 2017, detailing various irregularities, waste and deficiencies in the control environment at the SEC's data centers.[5]

Many Questions Remain Unanswered

The chairman's statement and subsequent testimony leave a number of critical questions unanswered, and in heavy questioning by senators at the Sept. 26 hearing, Clayton offered little additional detail. Several news outlets have reported that other SEC commissioners and senior leaders were not made aware of the breach until recently, and at the hearing Clayton expressed his belief that his predecessor, Mary Jo White, was equally unaware.[6] This revelation raises serious questions about the level of staff oversight on these issues, and whether lower level staffers deliberately concealed the event from their superiors and the commissioners.

Although the chairman's statement alludes to a defect in the EDGAR test filer system that permitted unauthorized access, it does not specify whether the intruders were limited to viewing test filings alone, or whether instead the defect created a backdoor to access other nonpublic information. Test filings by themselves often do not contain significant amounts of actionable information, but because the SEC concluded that the breach may have provided intruders a "basis for illicit gain through trading," the implication is that those intruders must have had access to more robust sets of information. EDGAR is not the only electronic documentary database the SEC maintains, but the SEC has not suggested that it has knowledge of intrusions into other systems.

Equally troubling is the fact that the breach was discovered not by any technological surveillance or countermeasures, but, according to Clayton, instead was revealed during a routine enforcement investigation. The SEC has not indicated which companies or industries were targeted, nor what categories of EDGAR filings were accessed. For example, unlike quarterly and annual reports that are eventually intended for a public audience, many companies communicate proprietary information that is never intended to be made public to the SEC staff by means of the EDGAR "correspondence" function. Was such correspondence compromised?

The SEC's Response

Clayton was overly contrite during the Senate hearing and adopted a penitent tone when interacting with senators at the oversight hearing. He indicated a number of remedial measures were in the process of implementation as well. The SEC continues to investigate the incident, and the chairman has asked the

agency's inspector general to conduct his own investigation, looking in particular at what led to the intrusion, the scope of nonpublic information compromised, and how the SEC should undertake future remedial efforts. The agency also intends to hire additional personnel, and will continue to revise its escalation protocols, presumably so that senior officials and the presidentially appointed commissioners are informed sooner.

Later in his testimony, Clayton indicated that the SEC seeks to spend $234 million on information technology as part of its 2018 appropriations request. In contrast, Clayton noted two prominent Wall Street banks that each spend more than $6.5 billion per year on IT. In fact, the entire annual budget for the SEC as a whole has remained flat in recent years at approximately $1.6 billion.[7]

Perhaps not coincidentally, on Sept. 25, 2017, the SEC reactivated a special enforcement unit devoted to cybersecurity. According to the SEC's press release,[8] the Cyber Unit will specialize in investigating:

- market manipulation schemes involving false information spread through electronic and social media;
- hacking to obtain material nonpublic information;
- violations involving distributed ledger technology and initial coin offerings;
- misconduct perpetrated using the dark web;
- intrusions into retail brokerage accounts; and
- cyber-related threats to trading platforms and other critical market infrastructure.

In many respects, the Cyber Unit resumes the specialized work of the prior Office of Internet Enforcement, which was originally organized in 1998 and disbanded as part of a broader reorganization of the Enforcement Division in 2009.

Next Steps

The EDGAR system itself is ancient by technological standards, having been first developed in the 1980s and periodically modernized over time with a series of regular modifications, updates and patches. At any rate, it is not surprising that such a system makes an attractive target for threat actors, not only due to its age and its bespoke nature, but also because of the treasure trove of information it contains. Assaults such as these on the SEC's systems were inevitable, and should only be expected to intensify in coming years.

Unfortunately, public companies have few options for safeguarding information in the EDGAR system before it is made public. There is no general exception from the obligation to file periodic reports

electronically through EDGAR and the SEC's other online filing systems, and the narrow hardship exemptions that permit paper filings on a limited basis would not be available in this situation. Still, there are a few steps registrants can take to mitigate the potential for misuse of information while it is in the SEC's systems.

Delay making test filings as long as possible. A test filing is a preliminary ping of the EDGAR filing system before the final "live" filing is submitted for the SEC's official use. Out of an abundance of caution, filing agents will often make test filings hours in advance of the actual "live" filing. To limit the amount of time an intruder into the SEC's systems will have to peruse test filing information, one possible solution is to delay making those test filings to the latest possible instant.

Similarly, do not make "live" filings the night before they are due. Because the EDGAR system does not publicly post filings made after 5:30 p.m., some registrants make the filing after working hours with the expectation they will post publicly to the system the next morning when EDGAR again goes live. While convenient, this process also gives an intruder into the SEC's databases exclusive access to the filing for whatever malicious purposes it may have.

Make greater use of confidential treatment requests in connection with "correspondence" filings. Registrants regularly communicate in writing with the SEC staff using the EDGAR correspondence function, particularly to respond to staff comments on periodic filings, proxy statements and registration statements. Indeed, the staff typically requires that such communications be filed electronically, and the staff's general policy is to make the correspondence publicly available through EDGAR shortly after conclusion of the review process. In other instances, the staff requests or requires additional explanatory or supportive material in connection with a review, which again must be furnished through the EDGAR correspondence function. This latter type of information is never intended to be made public, but nonetheless resides on the SEC's servers and provides a target of opportunity for a threat actor.

Notably, the SEC's rules for confidential treatment requests under the Freedom of Information Act generally permit registrants to redact sensitive financial or statistical information from the electronic EDGAR filing if they are accompanied by a paper filing without the redactions. These paper filings are typically not uploaded by the SEC staff to any electronic database and theoretically remain out of reach to cybercriminals. More liberal use of the confidential treatment process could be warranted to provide an extra measure of security for especially sensitive information.

Final Thoughts

In a series of cases in recent years, the SEC has brought insider trading and other related charges against hackers who made unauthorized access to computer systems to gain a trading advantage.[9] Absent some level of complicity in the unlawful activity, however, the SEC typically does not target the companies themselves that are the subject of insider trading by unaffiliated third parties. But the SEC has ratcheted up enforcement activity against registrants, typically broker-dealers or investment advisers, that have themselves been the subject of a breach when the affected company is perceived to have not met the SEC's requirements for data security.

The SEC will no doubt redouble its efforts to pursue parties that seek to benefit from their illicit access to computer systems for the purpose of gaining an informational advantage over the marketplace. The fog of

war present here — uncertain timelines, unknown threat actors, unclear reporting relationships, incomplete situational awareness, reputational harm — is found in many private sector data breaches as well. Having now been the victim, it remains to be seen whether this incident will soften the SEC's approach to cybersecurity enforcement against the companies themselves that are also all too often the victims of malicious cybercriminals.

Scott H. Kimpel is a partner in the Washington, DC office of Hunton & Williams LLP. Formerly counsel to SEC Commissioner Troy A. Paredes from 2008 to 2012, Kimpel brings in-depth knowledge of SEC policies, procedures and enforcement philosophy to each representation. He can be reached at (202) 955-1524 or skimpel@hunton.com.

[1] https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20

[2] https://www.sec.gov/news/press-release/2017-186

[3] https://www.gao.gov/mobile/products/GAO-17-469

[4] https://www.sec.gov/news/testimony/testimony-clayton-2017-09-26

[5] https://www.sec.gov/files/Audit-of-the-SECs-Management-of-Its-Data-Centers.pdf

[6] See https://www.law360.com/securities/articles/967594/sec-chairman-feels-bipartisan-heat-on-breach-disclosure?nl_pk=48ec22cf-c943-48ca-b231-bef63b3a6ff0&utm_source=newsletter&utm_medium=email&utm_campaign=securities

[7] https://www.sec.gov/foia/docs/budgetact.htm

[8] https://www.sec.gov/news/press-release/2017-176

[9] See, e.g., SEC v. Dorozhko, 574 F.3d 42 (2nd Cir. 2009)