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

SEC Failed To Heed Warnings Of Weak Cyber Defenses

By **Evan Weinberger**

Law360, New York (September 21, 2017, 12:38 PM EDT) -- A July government watchdog report warned the U.S. Securities and Exchange Commission that it had not fully put in place a system for monitoring cyber intrusions on its financial systems, even as the hack of a key electronic filing system for public company disclosures, which was revealed Wednesday, may have enabled insider trading.

The U.S. Government Accountability Office said a review of SEC cyber defenses conducted over the course of fiscal year 2016 found that the SEC did not "fully implement an intrusion detection capability for key financial systems" that the GAO had previously warned the commission about.

"As a result, SEC may not be able to detect or investigate some unauthorized system activity," according to the report, which included a review of SEC cybersecurity protocols ending on Sept. 30, 2016.

SEC Chairman Jay Clayton said the intrusion was detected in 2016 and that it "may have provided the basis for illicit gain through trading." (Law360)

The GAO's report, as well as other reported government watchdog concerns about the SEC's data security, came as the SEC was responding to a cyber intrusion of its Electronic Data Gathering, Analysis and Retrieval system that occurred at some point last year. SEC Chairman Jay Clayton revealed the breach Wednesday night.

According to Clayton's statement, the intrusion was detected in 2016 and that it "may have provided the basis for illicit gain through trading." The hack was the result of a software vulnerability in the test-filing component of the EDGAR system, Clayton added, noting that the weakness was promptly patched soon after it was detected.

However, the intrusion allowed hackers to access certain nonpublic information, although the agency doesn't believe personally identifiable information was exposed. The hack did not jeopardize the operations of the SEC or present a risk to the financial system, Clayton said.

The SEC chair did say that the commission learned in August that nonpublic information released due to the breach may have " provided the basis for illicit gain through trading."

“Our investigation of this matter is ongoing, however, and we are coordinating with appropriate authorities,” Clayton said.

The GAO report does not specify whether the SEC failed to put in place appropriate intrusion detection capabilities on the EDGAR system. It also does not mention the 2016 incident that Clayton referenced.

But Matthew Rossi, a former SEC enforcement attorney, said that if the commission did not have in place effective monitoring processes on its data systems, then even if the breach was patched as Clayton said, the SEC may not have been able to detect hackers going through data files and taking out information.

“Monitoring for system intrusion is something the SEC expects investment advisers, broker-dealers and others to be doing on their own systems," Rossi, now a partner at Mayer Brown LLP, said in a telephone interview.

It is unclear at this point whether the SEC did not disclose the 2016 incident to the GAO or whether the incident occurred after the GAO concluded its review last September.

Gregory Wilshusen, the GAO’s director for information security issues and one of the two lead authors of the report, told Law360 that he did not recall whether the SEC had disclosed the breach during the course of the GAO audit.

That could mean that the initial incident had not occurred by the time that the GAO completed the audit or that it was not believed to be serious.

“It could be that they detected it and did not tell us that they had this breach, or perhaps they thought it was not a significant breach,” Wilshusen said, noting that government agencies report tens of thousands of data breaches or attempted hacks each year.

The public version of the GAO report also does not single out EDGAR as a singular cause for concern, with Wilshusen noting that all of the agency’s information systems were included in the review.

“EDGAR was included in the scope of our review,” he said.

Former SEC Chair Mary Jo White and representatives of her current law firm, Debevoise & Plimpton LLP, as well as representatives for the SEC could not immediately be reached for comment.

The SEC's response to a draft version of the GAO report, written by Chief Information Officer Pamela C. Dyson, said that the agency concurred with all of the watchdog's recommendations and would work to implement them.

The GAO’s July report highlighted other problems with the SEC’s cyber defenses, including inadequacies in setting up firewalls on key data repositories, protecting passwords and authenticating the identities of users of those systems.

The GAO report found that the SEC had addressed 47 of 58 cybersecurity problems that were brought to the commission’s attention following a fiscal year 2015 audit. The report also found an additional 15 problems that “limited the effectiveness of SEC’s controls for protecting the confidentiality, integrity,

and availability of its information systems."

"While not individually or collectively constituting a material weakness or significant deficiency, these deficiencies warrant SEC management's attention. Until SEC mitigates these deficiencies, its financial and support systems and the information they contain will continue to be at unnecessary risk of compromise," the GAO report said.

The revelations of the EDGAR hack, and the SEC's inattention to concerns about its intrusion detection and identity authentication tools, may give companies that are under investigation the chance to argue for more leniency when the SEC challenges their cybersecurity protocols, said Jonathan Shapiro, a partner with Baker Botts LLP.

"They have a real glass house challenge on this," he said.

There have also been questions about the pace of the SEC's disclosures.

Attorneys cautioned that each disclosure has to be weighed against the individual facts and circumstances of each breach, noting that in many cases, the victim of a breach will wait until it has as many facts as possible before disclosing.

The assurances from Clayton that no personally identifying information was accessed as a result of the breach may have allowed the SEC to delay disclosure, Fenwick & West LLP partner Michael Dicke explained.

"That's a lot of the time what triggers notification," he said.

The revelations come at a sensitive time as the SEC develops the Consolidated Audit Trail, a new system for trade data currently in development by various exchanges. Clayton warned that could also be a target for hackers and criminals seeking sensitive information.

Companies that are providing information to the SEC may want added assurances that the commission is properly securing data.

"I think there are a number of people who are going to want to see more about that," said Mayer Brown partner Marcus Christian.

--Additional reporting by Ed Beeson. Editing by Christine Chun and Jill Coffey.

Update: This story has been updated with more details about the report and the breach.
