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 Takes Walk In Businesses' Shoes With Database Hack

By **Allison Grande**

Law360, New York (September 22, 2017, 9:58 PM EDT) -- The U.S. Securities and Exchange Commission provided companies with a crash course in what to do — and what not to do — when it recently revealed that its electronic public document filing system had been hacked last year.

SEC Chairman Jay Clayton announced on Wednesday that the 2016 cyberattack potentially exposed securities data that could have led to the theft of investor dollars through insider training.

The revelation left lingering questions about whether the SEC before the attack exercised the same level of data security it demands of firms and investors it regulates, not to mention the yearlong lag in addressing and disclosing the breach. And how the commission continues to respond to the data breach after a rocky start, as some attorneys say, could determine whether it redeems its moral authority to continue aggressive cybersecurity enforcement.

"It's always an arms race, and the question is not perfection; it's whether you're trying your best to secure data and inform capital markets about what was hacked and what you're doing to fix that," said Seward & Kissel LLP partner Marlon Q. Paz, who previously served in the SEC's Division of Trading and Markets. "I hope the SEC does that and leads by example because right now, there is a danger that the SEC could lose its moral leadership if it doesn't act in a manner that they expect registrants and regulated entities to behave."

How to best disclose cyber risks and respond to a cyberattack has plagued public companies since 2011, when the SEC issued staff-level guidance that pushed these businesses to be more upfront about cybersecurity in their public filings. Since then, the commission has stepped up pressure by conducting examinations to assess cybersecurity readiness and response procedures and indicating that an enforcement action for inadequate disclosures could be on the horizon.

"Disclosures have been a huge challenge for companies because pursuant to the 2011 guidelines, companies are not supposed to disclose in a boilerplate way that's not transparent, but you're also not supposed to disclose details that can provide a road map for future attackers," said John Reed Stark, the president of cybersecurity firm John Reed Stark Consulting LLC and former chief of the SEC's Office of Internet Enforcement.

Although it's unclear yet why the SEC chose to wait so long to disclose the data breach and why it didn't mention the incident until more than a dozen paragraphs into a lengthy statement Clayton issued late

Wednesday about the commission's overall cybersecurity efforts, "based on what I've seen so far, I don't think this response will be held up as a best practice," said Marcus Christian, a Mayer Brown LLP cybersecurity and data privacy partner and former federal prosecutor.

While some aspects of the disclosure raised eyebrows, including that it was detected in 2016, but the SEC waited to go public with it until after it discovered last month that the compromised data may have been used to make illicit trades, there were positives that companies could derive from the way the SEC has handled the incident so far, including that the chairman himself delivered the news and that he provided details about the commission's collection and use of data and its key cyber risks more generally, experts say.

"The statement is notable for its candor and its robust and comprehensive presentation," Stark said, noting that the commission's disclosure that hackers may have used the nonpublic data available in its filing database, known as EDGAR, for insider trading seemed to be the "worst-case scenario." Companies that tend to be more "cautious and guarded" in their disclosures don't always announce such possibilities, he said.

Although observers identified some stumbles with the SEC's initial disclosure, where the SEC goes from here will be important for companies to watch, experts say.

"The SEC has a chance here to be a leader in breach response protocol and show that this is how you disclose a cyber intrusion event," Paz said. "But that will depend greatly on how Chairman Clayton treats the assessment that he mentions in his statement and how the commission follows up."

While the SEC has said it is conducting an internal investigation, the incident is also likely to attract scrutiny from external sources, which attorneys say will bear watching.

"The incident again raises the question of who regulates the regulators," Shook Hardy & Bacon LLP data security and privacy group chair Al Saikali said.

The SEC won't face a regulatory probe the way a business might, but executive branch officials and members of Congress are likely to question the commission about whether more could have been done to fortify systems against hackers and why it took so long for the incident to come to light, experts say.

Hours after the breach was disclosed, news emerged that the U.S. Government and Accountability Office had warned the SEC in a July report that it had not fully implemented an intrusion detection capability. The government watchdog is likely to be charged with taking a closer look at the SEC's cybersecurity safeguards in the aftermath of this hack, Intelligize CEO Todd Hicks noted.

The Trump administration, which in May issued an executive order instructing federal agencies to assess cybersecurity risks and share threat information in order to better safeguard federal networks and infrastructure, also is expected to pressure agencies like the SEC to improve their cyber protections, as will members of Congress, experts say.

Sen. Mark Warren, D-Va., has already spoken out about the incident, saying that it "shows that government and businesses need to step up their efforts to protect our most sensitive personal and commercial information," and Clayton is expected to undergo intense questioning about the hack at a previously scheduled SEC oversight hearing before the Senate banking committee on Tuesday.

"This should be yet another wake-up call to hurry up and solidify federal defenses against cyberattacks, although honestly, the federal government has had more wake-up calls than a sleepy teenager on a Monday morning," Pillsbury Winthrop Shaw Pittman LLP partner Brian Finch said. "What really matters here isn't that an attack occurred and succeeded. What matters is how long it took to discover the attack and remedy it."

The SEC's ability to protect the sensitive data it holds is important not only to investment markets, which rely on trades being made only on public data, but also to companies, which, "given the types of information they submit to the SEC, would expect it to be held with Fort Knox-like security," Christian noted.

While information will continue to flow to the regulator, businesses may choose to start approaching the SEC like any of its third-party vendors, which are routinely asked what they are doing to protect the sensitive data that is being handed over to them, according to attorneys.

"That's a fair question to ask the SEC now," Paz said.

It won't be a one-way street, though. Despite the security setback, attorneys don't anticipate that the SEC will shrink from its obligations to police corporate data security anytime soon.

"It's unlikely that this incident is going to change the commission's mandate or ability to continue to investigate security incidents and disclosures surrounding such events, although it is likely to give the commission a better perspective on what the companies they're investigating may have experienced as well," Hunton & Williams LLP attorney Brittany Bacon said.

In fact, experts predict that the hack could put even more pressure on the SEC to strengthen its inquiries into what cybersecurity issues companies are experiencing and how they are disclosing them.

"The SEC mandate is to level the playing field in the open market," Hicks said. "This breach could call that ability into question and require the SEC to focus more on cybersecurity to ensure activity within the free markets remains just and fair."

Just because the SEC itself may have had some security failings, that "doesn't mean they can't regulate what other parties are doing," according to Dechert LLP partner David Vaughn.

Whether the government has attained the level of cybersecurity that it expects from others “is a little bit beside the point," Dechert partner Tim Blank added.

"The government certainly would strive to be there, but their job is to make sure that the investing public is protected,” he said.

In scrutinizing companies, the SEC will continue to "expect companies to adopt, maintain and update sophisticated cybersecurity measures," according to Stephen Crimmins, an attorney with Murphy & McGonigle PC and a former SEC enforcement attorney.

"At the same time, the SEC will understand that no defense can be absolute, and that companies demonstrating best efforts should not be sanctioned," he added.

Given the commission's likely focus, companies would be best served to focus on answering questions

such as whether there is an incident response plan in place that, as Stark put it, allows for "a rapid, candid, transparent and independent response"; whether companies are taking steps to protect against and mitigate the risk associated with cyber events; and what their actual response looks like, attorneys say.

"What companies should think about when a breach happens is, if they're talking to the government three months down the line, what story do they want to tell?" said Brenda Sharton, chair of Goodwin Procter LLP's privacy and cybersecurity practice and its business litigation practice. "Then, they should take those steps to be able to tell it."

While the SEC hack drives home the reality that anyone, even those that are tasked with regulating cybersecurity, can be hit by a cyberattack, a conclusion that shouldn't be drawn from the incident would be that nothing can or should be done to address this growing threat, Christian noted.

"The wrong message would be that if this is happening to everyone, let's not invest in cybersecurity," he said. "This is another high-profile reminder about how important it is to take cybersecurity seriously and make sure that they have the proper administrative, physical and technical controls in place."

Making cybersecurity a top priority gains added urgency in light of the SEC hack being only the latest in a long line of intrusions that have affected a diverse list of public and private sector entities, including Target, the Office of Personnel Management, the Internal Revenue Service and most recently, Equifax, which earlier this month disclosed a massive breach that compromised the personal data of 143 million consumers.

"Investors and firms in this area have to know this is not the end," said Ballard Spahr LLP partner David Axelrod, a former supervisory trial counsel at the SEC's Philadelphia regional office. "Unfortunately, we are going to live in an area where these things are going to become the norm, and we are going to see large-scale intrusions on a pretty frequent basis."

--Additional reporting by Tom Zanki. Editing by Christine Chun and Catherine Sum.

All Content © 2003-2017, Portfolio Media, Inc.