LAW360

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

Yearlong Breach Probe Puts SEC In Businesses' Shoes

By **Ben Kochman**

Law360 (June 6, 2023, 8:29 PM EDT) -- The U.S. Securities and Exchange Commission's yearlong investigation revealing that an in-house data breach had a far deeper impact than previously believed could give the agency — which is finalizing closely watched new cyber incident reporting rules — insight into the challenges faced by cyberattack victims.

In a Friday statement, SEC officials said that an internal error that allowed employees in the agency's enforcement division to improperly access documents drafted by a separate staff for adjudicating cases in 2017 may have affected nearly 90 of the agency's cases, far more than the two cases the agency had originally identified in April 2022 as being impacted.

The new disclosure, including a statement in which the SEC said that "we deeply regret that the agency's internal systems lacked sufficient safeguards" to protect adjudication documents, resembles the responses made by several businesses in recent years that have identified deeper damage from cybersecurity episodes after investigations that routinely can take months or years, cybersecurity experts say.

Friday's update also came as the SEC works to finalize data security incident reporting rules that are set to call on companies to report "material" episodes to authorities within four days. The regulator has called for businesses to determine whether episodes are material "in as prompt a manner as feasible," while data breach responders and industry lobbyists have called for cyberattack victims to have more time to investigate incidents before reporting them to investors and the public.

It remains to be seen whether the SEC's own breach investigation will have any impact on the breach reporting requirements that the agency ultimately rolls out for businesses. But cybersecurity attorneys say they hope the agency's firsthand knowledge of how information can trickle out slowly about breaches could lead to regulators having a greater understanding of why companies are unsettled by the prospect of divulging key details about breaches soon after they occur.

"Whether you are the SEC or a company that is the victim of a cyberattack, it's just not possible to conduct very fast investigations into cyber incidents and to come to a reliable and accurate conclusion about what happened," said Haima Marlier, a former official in the SEC's New York office who is now a partner at Morrison Foerster LLP.

"The SEC's own timetable shows that this is true for them too," Marlier added. "Just like it took the SEC some time to really get its arms around the scope of its incident, all victims of cyberattacks need that

time to truly understand what is going on."

The SEC, which did not respond to a request for comment Tuesday, has made an effort to tackle cybersecurity issues more aggressively under the leadership of Chair Gary Gensler. The agency's bid to carve itself a growing role as a cybersecurity watchdog has led to it taking a far more adversarial role with businesses on cybersecurity issues compared to other agencies, like the Cybersecurity and Infrastructure Security Agency, which have pitched companies on disclosing cyber incidents as part of a mutually beneficial exchange of information.

In January, the SEC fired the first salvo in what has become a massive legal battle by urging a D.C. federal court to grant the agency an order that would force Covington & Burling LLP to reveal which of its clients were impacted by a 2020 cyberattack on Microsoft Exchange email servers used by thousands of companies across the globe.

Covington has said that complying with the SEC's order would breach its duties to keep client communications privileged. More than 80 of the world's biggest law firms have agreed, arguing that the SEC is aiming to violate "one of the oldest and most inviolate principles in American law" while offering "vague speculation" for why it needs the information.

SEC officials say they are seeking the information in both the Covington case and from companies recovering from data breaches in order to protect the market from potential federal securities fraud. But cybersecurity attorneys say they are hoping the agency's own experience investigating its breach will cause the agency to focus less on how quickly businesses report episodes and more on whether the information they disclose is accurate and if companies have appropriate protocols in place for responding to cyber episodes.

"The SEC now has firsthand experience of what it is like to try to investigate a data security incident, and how even with the best of intentions and resources devoted to it, it can take a long time before you know the full extent of the situation," said Alexander "Sandy" Bilus, the co-chair of Saul Ewing LLP's cybersecurity and privacy practice.

Supporters of the SEC's breach reporting rules, however, say that the agency should push ahead with its reporting requirements, which could provide consumers with a valuable opportunity to know about data thefts and take steps to protect themselves.

"Notification can make the difference between identity theft that inflicts major financial losses and a swift response that results in minimal harm," said Stephen Hall, legal director of the financial watchdog group Better Markets.

"That's what the SEC's proposed rule does. It requires financial firms to notify breach victims so that they can take prompt action to protect themselves from the potential consequences," Hall said. "We urge the SEC to finalize the proposal without weakening any of its elements."

--Additional reporting by Jessica Corso. Editing by Jill Coffey.
