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

Critics Of SEC Data Breach Rules Question 4-Day Deadline

By **Ben Kochman**

Law360 (June 10, 2022, 8:24 PM EDT) -- The U.S. Securities and Exchange Commission's plan to apply the same four-day deadline that companies have to report straightforward news like naming a new CEO to the more murky world of data security episodes could confuse investors or interfere with investigations, breach response lawyers say.

In more than 130 comments left last month on the SEC's preliminary rules, which would require companies to disclose "material" breaches within four days, law firms, businesses and lobbyists argued that cyberattack victims should have more time to investigate incidents before reporting them to investors and the public.

The agency **proposed in March** that publicly traded companies disclose cybersecurity incidents through Form 8-K, which covers material developments that occur between a business's quarterly or annual filings, such as declarations of bankruptcy or entering into major sales contracts.

But mandating that companies apply the same four-day reporting standard to disclosing active cybersecurity episodes, using public statements often cited in post-breach lawsuits, will likely leave investors with more questions than answers and could jeopardize probes by tipping off attackers that a victim is aware of their activities, breach victim advisers claim.

"In those early days, a company's response to a cybersecurity event is very much a fog of war environment," said Hunton Andrews Kurth LLP partner Scott Kimpel, whose firm was among those that commented on the SEC's proposal. "Instead of trickling information out to investors piecemeal, why not wait until you've done a more thorough job and have a better understanding of the incident?"

SEC leadership, in pushing for the rules, have said investors would benefit from "timely and consistent disclosure" of data security incidents given the massive impact cyberattacks can have on businesses. But law firms and lobbyists that represent breach victims say the four-day deadline could hamper attempts to blunt the impact of intrusions, including by convincing attackers who know they've been detected to steal more data.

"If a company identifies that it has been victim of a cyberattack and has just four days to report that information, that might provoke a malicious actor to expedite its activities," said Henry Young, policy director at BSA: The Software Alliance, a software industry trade group that also weighed in publicly on the SEC's plans. "I just don't think that promulgating an inflexible rule will have good results for the cybersecurity of registrants."

Attorneys at Wilson Sonsini Goodrich & Rosati PC, in their public comment on the rule, brought up

another potentially damaging scenario for breach victims. Tipping off sophisticated nation-state-backed attackers that they've been detected could cause them to abandon hacking efforts for now, yet leave open other, undiscovered points of entry that they could use to infiltrate a company later, the firm said.

"The commission does not consider whether the disclosure of an ongoing incident prior to remediation could cause further harm to the company and its shareholders," Wilson Sonsini's lawyers wrote.

In interviews with Law360, industry attorneys said SEC incident disclosures produced within four days are likely to be far more opaque than conversations with other government agencies like the U.S. Cybersecurity and Infrastructure Security Agency, which has urged the private sector to view it **as a partner** in efforts to curb hacking rather than a source of anxiety in terms of enforcement actions.

Because the SEC reports would be public, and a full analysis of a data breach can take weeks or months to complete, companies are likely to be overly cautious with what they disclose, said John Reed Stark, a former SEC internet enforcement chief who now runs his own data breach response and digital compliance firm, John Reed Stark Consulting LLC.

Company statements in public filings about cybersecurity are often cited in lawsuits **filed after data breaches**, with investors or consumers claiming that businesses misled the market about the extent of a breach.

"The more that you say immediately after a data security incident, the more likely it is that you say something that is going to turn out to be false," Stark told Law360.

Other critics of the SEC's proposed four-day deadline included Davis Polk & Wardwell LLP, whose attorneys argued in a public comment that the rules would likely cause companies to report breaches "as soon as possible without the benefit of a considered analysis of the impact of the incident."

Energy giant Chevron Inc., meanwhile, pushed the commission to provide an exception in cases where a business is cooperating with an active law enforcement investigation or negotiating with cybercriminals to recover "critical corporate assets" affected by a ransomware attack.

Hunton's SEC comment homed in on another **thorny question** facing regulators or lawmakers in the cybersecurity world — how to define a "material" cybersecurity breach in the first place.

The law firm pushed the SEC, which did not respond Friday to a request for comment, to change its definition of an incident to cover breaches that have "adverse effects" on a company's data or networks, rather than episodes that merely "jeopardize the confidentiality, integrity, or availability" of systems or information.

"There needs to be more specificity about what it is that we are reporting," Kimpel told Law360. "The real inquiry should be based on measuring something that does happen, rather than on a situation where something might happen."

--Additional reporting by Tom Zanki. Editing by Kelly Duncan and Lakshna Mehta.