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

Feds Aim For More Insight On Hacks With Maze Of Policies

By **Ben Kochman**

Law360 (August 12, 2022, 9:53 AM EDT) -- As U.S. federal agencies push for more visibility into cyberattacks with a fast-developing patchwork of reporting rules, industry observers are keeping a close eye on how broadly the new laws will define covered entities and how quickly companies will be required to notify officials.

The U.S. Securities and Exchange Commission and the Cybersecurity and Infrastructure Security Agency, or CISA, are each mulling the details of breach reporting rules expected to have a deep impact on the way publicly traded companies and critical infrastructure operators respond to attacks. Regulators overseeing the banking, telecommunications and critical pipeline industries, among others, have also jumped into the breach notification law fray with their own policies.

The new crop of federal breach reporting laws reflects authorities' change in mindset after several high-profile attacks on critical infrastructure in recent years, industry attorneys say. Rather than focusing just on whether personal data was accessed or stolen during an incident, the new wave of federal laws covers a broader swath of episodes that pose a danger to networks or materially impact a victim's operations.

"There's been a realization that our old breach notification laws don't do enough to cover new and emerging threats," said Jami Vibbert, a partner in the privacy and data security practice at Arnold & Porter. "Regulators are recognizing that a lot of harm can come from cyberattacks that has noting to do with personal data and privacy."

Here, Law360 takes a closer look at the federal cybersecurity policies worth following in the second half of 2022.

SEC's Breach Report Proposal Sparks Industry Blowback

The SEC is scheduled to vote in April 2023 on a final version of new rules that as proposed in March will require publicly traded companies to disclose cybersecurity incidents within four days.

Until then, it will be worth watching how the agency addresses **concerns raised** by the private sector that applying the same 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 government investigations.

Among the suggestions made in more than 130 public comments left earlier this year on the SEC's preliminary rules were to expand the reporting deadline, exempt reporting in cases involving government investigations, and scale down the scope of data companies will be asked to provide about their incident response plans.

"The requirements for companies to disclose features of their cybersecurity risk infrastructures, if taken literally, could provide a road map for cybercriminals to attack those companies," said Haima Marlier, a former official in the SEC's New York office who is now a partner at Morrison Foerster LLP.

Given the crush of comments mentioning a law enforcement exemption, it's likely that the agency will at least "seriously consider" adding such a provision, Marlier added.

Companies Seek Clarity on Scope of CISA Breach Rules

CISA officials have attempted to position themselves as a partner to the private sector in efforts to curb hacking, pledging not to use incident reports to punish breach victims.

For now, the agency is pushing businesses to voluntarily share information about data security episodes. But legislation passed in March will eventually require critical infrastructure operators to report "substantial" data security incidents to the agency within 72 hours, and alert it within 24 hours of making a ransomware payment.

The Cyber Incident Reporting for Critical Infrastructure Act, however, won't come into effect for at least the two years CISA has been given to finalize rules on how the law will work.

The law specifies that organizations in 16 critical infrastructure sectors will be subject to the new reporting rules. But industry attorneys say that they are eagerly awaiting further guidance about whether subcategories in business sectors like software development, life sciences and hospitality will also be considered "critical" by CISA.

"There is a sense among the business community that we will have to report faster and more robustly, but the critical infrastructure bill was written so broadly that it has left many companies wondering whether they will be included," said Aaron Charfoos, a partner in the privacy and cybersecurity practice at Paul Hastings LLP.

Industry-Specific Regulators Try Their Hand at Mandating Breach Disclosure

Regulators in the banking, pipeline and telecom industries, among others, have issued their own versions of breach reporting rules in recent months, adding to the patchwork of disclosures that cyberattack victims may face after an incident.

In May, for example, a federal rule went into effect that will require U.S. banks to alert authorities about confirmed cybersecurity episodes within 36 hours. The Federal Reserve, Federal Deposit Insurance Corp. and Office of the Comptroller of the Currency used a new, narrowed definition of a cybersecurity "incident," after lobbyists claimed that officials would be overwhelmed with notifications for incidents that may not be as dangerous as the type of hacks the rule intended to address.

The Transportation Security Administration, meanwhile, recently said that it had reissued a security directive ordered in the wake of the Colonial Pipeline Co. ransomware attack amid industry criticism.

The new version of the directive pushed back the deadline for reporting incidents from 12 to 24 hours, and allows pipeline companies more wiggle room on how to meet a set of cybersecurity standards.

The Federal Communications Commission is also considering issuing new rules to make telecom customers more quickly aware of personal data breaches under a plan floated in January. FCC Chair Jessica Rosenworcel said at the time that she is pushing to remove a seven-day waiting period for businesses to notify customers about personal data breaches, and to require companies to notify the FCC along with the FBI and U.S. Secret Service of such events.

With federal breach disclosure rules continuing to proliferate, businesses are likely to push lawmakers to harmonize aspects of the regulations in order to simplify the reporting process, industry attorneys say.

"The private sector has an appetite to create some simplicity and consistency in these rules," said Alex Iftimie, a partner in Morrison Foerster's privacy and data security group. "They are looking to make sure that there is one door to walk through and a consistent set of standards to follow."

--Additional reporting by Christopher Cole. Editing by Daniel King.
