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 Rules Making Cyber Disclosures Public May Raise Risk

By **Allison Grande**

Law360 (August 8, 2023, 10:21 PM EDT) -- The U.S. Securities and Exchange Commission's recently finalized cybersecurity rules bring out of the shadows disclosures that companies have typically been able to keep private or reveal in a controlled manner, ramping up the potential for increased attention from regulators and shareholders — as well as hackers.

During its July 26 open meeting, the commission voted 3-2 to finalize a rule that it had initially floated last March requiring public companies to make incident-specific disclosures of significant cybersecurity breaches within four business days of their determining that the incident is material, and annual disclosures about companies' cybersecurity risk management, strategy and governance practices.

While many public companies already have similar obligations under a broad patchwork of laws and regulations that have popped up at the state, federal and international levels in recent years — including the requirement for certain financial institutions to report breaches to the New York Department of Financial Services within 72 hours after they've determined a breach has occurred — the public nature of the SEC-mandated disclosures make them a "game changer," noted Justin Herring, a partner at Mayer Brown LLP.

"It's not so much the four-day reporting window that's the critical issue," said Herring, who prior to joining the firm in April was the executive deputy superintendent of the cybersecurity division at NYDFS. "It's the public disclosure that makes these regulations fundamentally very different. It takes away companies' ability to control the timeline."

Under existing breach reporting regimes, companies typically make early disclosures privately to regulators and are given more time to assess the situation before they need to go public with details about the incident or their cybersecurity posture. But under the SEC's rules, which take effect in December, this process is accelerated, with companies likely needing to take additional steps to ensure employees, vendors and other key partners aren't hearing about the incident for the first time in a public filing, according to attorneys.

"This is more than just a disclose-to-the-SEC rule," Herring said. "It's a disclose-to-everyone rule."

Pushing companies to publicly reveal data breaches at a juncture when they often don't have a clear and complete picture of the incident and to annually update the public on its cybersecurity posture will likely draw increased scrutiny from not only the SEC, which is expected to aggressively enforce its rule, but also shareholders and bad actors, who will now have greater insight into what's occurring inside a

company, according to attorneys.

"The cyber risk disclosure process is intended to assist non-cyber experts in making investment decisions, but it's also likely to assist cyber criminals by informing them about companies' cybersecurity posture and resilience, and plaintiffs counsel will also likely be looking at whether disclosures about risk management programs are accurate," said Shardul Desai, a partner with Holland & Knight LLP who handles cybersecurity and data privacy matters. "That raises the concern that the rule is a little shortsighted in creating additional significant risks, with some marginal gains for investors."

In finalizing its rule, the SEC appeared to respond to some of these concerns by pulling back on a few of the broader mandates in its initial proposal. These changes included requiring companies to disclose only the material impacts of a cybersecurity incident — including its nature, scope or timing — rather than more granular details, and scrapping the mandate for companies to have a board member who is a cybersecurity expert.

While attorneys say these adjustments provide some welcome relief and more flexibility for companies, they weren't enough to ward off criticism from the two Republican commissioners, who voted against finalizing the rule. During the meeting, Commissioner Hester Peirce argued the regulations went beyond the agency's authority to regulate disclosure obligations by attempting to also mandate companies' cyber defenses, and that the granular nature of companies' disclosure obligations had the potential to give hackers valuable insight into how businesses respond to and manage cyberattacks.

The U.S. Chamber of Commerce has also spoken out about the impact and potential "overreach" of the new regulations.

Christopher Roberti, U.S. Chamber senior vice president for cyber, space and national security policy, noted that the rule "sharply diverges" from the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which made clear that incident reporting to the government "should occur confidentially and in a protected manner." It's also at odds with President Joe Biden's push in his recent National Cybersecurity Strategy for federal agencies to harmonize and streamline new and existing cybersecurity regulations, Roberti said.

The rule therefore throws a wrench in efforts to establish a much-needed confidential reporting strategy that ensures that companies can remediate incidents before they go public, according to Roberti.

"The U.S. Chamber has long advocated for a cohesive, aligned and protected regulatory framework for cyber risk management and continues to have grave concerns about the potential impact of the rule as finalized by the SEC," Roberti said, adding that the chamber planned to "continue to carefully evaluate the impact of this rule and our options going forward."

However, despite these internal and external concerns, the SEC is expected to aggressively enforce its new rule, which builds on many of the disclosure principles that the agency has long advocated for in the cybersecurity arena, attorneys noted.

"The underlying principles and philosophy behind this rulemaking are nothing new in the sense that the SEC has signaled for well over a decade that there could be disclosure obligations for not only cyber risk but also cyber incidents to the extent that they are material," said Erin Martin, a partner at Morgan Lewis & Bockius LLP who worked in the SEC's Division of Corporation Finance for more than a decade.

"So what this rulemaking is doing is codifying that position that cyber events are material and disclosure is warranted on a prompt basis, and that mandate does make it easier for the commission to establish where someone has or has not met the basic requirement of disclosure for material events and creates the potential for elevated enforcement," Martin added.

Given that the SEC has "repeatedly" listed cybersecurity as one of its top enforcement and examination priorities and in 2017 established a dedicated cyber enforcement unit, the agency is sure to pay close attention to how companies are complying with their enhanced cyber disclosure obligations now that there are formal rules, attorneys say.

"The SEC is gaining experience and continuing to focus on these cyber issues, so we're expecting to see increased enforcement activity based on these rules, which mark a shift in how companies are expected to approach incident reporting," said Kate Hanniford, a partner on the privacy, cyber and data strategy team at Alston & Bird LLP.

One area that's likely to be of particular interest to the SEC is how companies go about determining "as soon as reasonably practicable after discovery" of a security breach whether that incident is "material," setting in motion the breach reporting clock.

"Given the number of cybersecurity incidences that happen every day, the threshold issue for most companies will be determining when an incident or series of related incidences hit the materiality threshold that triggers the four-day reporting requirement," said Jane Norberg, an Arnold & Porter partner who served as a senior officer in the enforcement division at the SEC.

While the SEC said that the materiality standard companies should apply in evaluating whether a Form 8-K public disclosure is warranted should be "consistent with that set out in numerous cases addressing materiality in the securities law," experts say the results of that analysis could be open to interpretation and second-guessing by the SEC, especially in the earliest stages of enforcing the new regulations.

"This is really going to force companies to assess materiality more quickly than normally in these type of events, and that standard may be difficult for companies and SEC staff to apply because it's inherently subjective," said Matt Franker, a partner at Covington & Burling LLP. "Prior to the effective date, at least initially, we'll probably see more 8-K filings than we would have in absence of the rules."

These filings will be prompted by companies not only erring on the side of caution in initially disclosing incidents, but also by the requirement that they need to make another disclosure if they learn additional material information during the course of the breach investigation.

"It's quite common for companies to realize a month into investigating an incident that the compromise went beyond what it originally thought. This can put the company back on the four-day disclosure clock and then have to repeat the process," said Herring, the Mayer Brown partner. "This is going to add to the fire drill for companies dealing with an incident, and in many cases, if it's a close call, companies are going to find that they should disclose."

Given the demands of the new regulations, companies shouldn't delay in ensuring that they have the policies and procedures in place to make swift materiality assessments and report incidents well in advance of a significant cyberattack, attorneys say.

"Being prepared and having a game plan is going to be really important to effectively executing on the

new rule's reporting time frame," said Dave Brown, a partner in the corporate transactions and securities group at Alston & Bird. "The rule makes clear that the SEC is really focused on changing the disclosure dynamic and shifting the way companies view cyber incidents and their seriousness."

Companies will also need to ensure that they have processes and procedures in place to not only be able to quickly conduct post-breach materiality assessments, but also to fall into step with their additional obligations to annually inform investors about the company's efforts to assess, identify and manage material risks from cybersecurity threats and what role management and the board play in overseeing this work.

"The SEC's rule moves cybersecurity processes and personnel even more into the mainstream of a public company's operations and governance," noted Ronald Lee, a partner at Arnold & Porter.

For companies that have made managing cybersecurity risk a board-level priority, the new corporate governance reporting requirements shouldn't provide much additional burden, noted Gerry Stegmaier, a partner in the tech and data group at Reed Smith LLP.

However, "organizations with less mature security programs may have a more difficult time, as the distance between the server room and the boardroom often remains great in such companies," Stegmaier noted, adding that the new regulations are primarily focused on driving "greater attention to transparency and consistency of disclosure."

For all companies, ensuring that their cyber disclosures are tailored in such a way that they meet the SEC's requirements without providing ammunition for future cyberattacks or legal backlash will also be vital.

"Once these disclosures are out in the open, not only are the SEC and investors reading them, but they'll also be other regulators, customers, business counterparts, litigants and others out there monitoring and scrutinizing what's been said," said Caleb Skeath, a partner at Covington. "So companies need to consider what they're disclosing and how they're framing it not only from the point of view of meeting the SEC's requirements, but also from these other perspectives to make sure they're not opening themselves up to new areas of risk and scrutiny."

While Democratic SEC Commissioner Jaime Lizárraga stressed last month that the final rule doesn't require specific technical information that would give bad actors a road map for future attacks, concerns still exist that the information that companies are required to provide about the timing, nature, scope and likely impact of incidents, as well as how companies are guarding against these threats, can prove to be helpful to increasingly sophisticated hackers and litigants.

"We're seeing an increasing amount of data breach litigation after an incident, and these disclosures could provide shareholders' counsel with a road map to take what the company has said about its cyber program and procedures and allege in the event of a material cyber event that the company wasn't doing that," noted Cara Peterman, a partner in the securities litigation group at Alston & Bird.

Additionally, companies need to ensure that their processes and disclosures are consistent with the growing patchwork of cybersecurity regulations around the world, which include the New York Department of Financial Services rules; laws in all 50 U.S. states that mandate notifying regulators and affected individuals of breaches of varying timelines; and the requirement for companies to report data breaches to European Union authorities within 72 hours of becoming aware of the incident.

Although the White House and others have called for greater harmonization of these disclosure requirements, the SEC said existing regulations and laws like the Cyber Incident Reporting for Critical Infrastructure Act of 2022 — which requires companies to confidentially report most cyber incidents to federal officials within 72 hours of discovery and ransom payments within 24 hours — would "not effectuate the level of public cybersecurity disclosure needed by investors in public companies."

"What we're seeing with the SEC rules is part of a broader trend of different regulators writing cyber rules within their spheres of authority," said Herring of Mayer Brown. "That's creating a more complex environment for companies that over the last four to five years have seen all these new cyber regulations emerge, and it's only going to become more complex with more regulations still to come."

--Additional reporting by Sarah Jarvis. Editing by Alanna Weissman and Michael Watanabe.
