LAW360 Insurance Authority

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

Cyber Reporting Requirements Keep Policyholders On Toes

By **Daniel Tay**

Law360 (March 25, 2022, 4:11 PM EDT) -- Recent laws and proposed regulations requiring disclosures of cyber incidents could encourage increased cyber resiliency but could also result in increased litigation, compliance costs or penalties, meaning policyholders should reexamine their cyber and directors and officers policies to ensure adequate coverage.

President Joe Biden's recent signing of the Cyber Incident Reporting for Critical Infrastructure Act and the U.S. Securities and Exchange Commission's proposal requiring stricter disclosures of cybersecurity and cyber incidents for public companies reflect continued governmental and regulatory interest in more cybersecurity regulation. The increased disclosure requirements are likely to further push companies to increase their cyber resiliency.

"They're further advancing a goal that's already in place, and they're consistent with what I've seen as developing in both the cyber insurance market as well as the law in terms of what is expected of companies," Joshua Mooney, a partner with Kennedys representing insurers, told Law360, referring to the act and the proposed rule.

The act, signed by Biden on March 15, **represents a major move** by federal lawmakers to clamp down on cyberattacks, including increasingly prevalent threats from nation-states like Russia and China. It will require a broad range of companies that power the nation's critical infrastructure to report "substantial" cyber incidents to the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, or CISA, within 72 hours and to disclose payments made in response to ransomware attacks within 24 hours.

CISA will have the authority to undertake rulemaking to determine the exact parameters of covered incidents and entities, subject to minimum standards laid out in the law.

The SEC's rule, proposed March 9, **would require public companies** to disclose breaches within four days upon determining that an incident was material and update prior disclosures as needed. The rule as proposed would also require companies to periodically describe their risk management strategies, and report whether management or directors have cybersecurity expertise, among other things.

The act and the proposed rule are likely to "push down" increased cyber resiliency to smaller third-party vendors working with entities required by the act or the proposed rule to make reports, as they both provide that cyber incidents at third-party vendors can implicate notification requirements, Mooney added. As a result, the collective level of cyber resilience for all companies in the U.S. may rise, not just the resilience of companies required to report by the act or proposed rule.

The focus on cyber resiliency could result in decreased risk profiles for policyholders, which in turn could result in lower premiums for cyber policies. However, a "softer" cyber market, meaning one with increased capacity and lower premiums, is not guaranteed even with a heightened level of resilience, Emily Garrison, a partner at Honigman LLP who represents policyholders, told Law360.

"To the extent that the government's able to have a significant impact on the amount of incidents that are happening, hopefully it would open up the market because there'd be less incidents and less claims, but I'm not sure," Garrison told Law360.

For now, insurers might not be willing to provide additional coverage until they are sure of the impacts of the law and proposed rule, she added.

While governmental disclosures may incentivize good cyber hygiene, they could also result in increased litigation risks for policyholders if implemented poorly. This means companies should review their cyber policies to determine the extent of their coverage, particularly for costs of complying with reporting cyber events or the costs of government investigations or penalties stemming from an alleged reporting failure, Jim Carter, partner at Blank Rome LLP who represents policyholders, told Law360.

"With respect to the SEC proposed rule, in particular, companies should look to see whether or not the securities-related exclusion, which appears in many policies, contains an exception that would preserve coverage," Carter said.

Currently, the Cyber Incident Reporting for Critical Infrastructure Act contains several liability protections for entities that report events to the CISA, including providing that companies can't be sued or face regulatory investigations based solely on information submitted through a mandated report. However, the SEC's proposed rules in their current form lack such protections.

Depending on the final rule's disclosure requirements, the information disclosed by companies could be used against them to "ratchet up the potential damages arising out of a cyber event," Mark Camillo, CEO of cyberinsurance risk mitigation company CyberAcuView, told Law360.

"You could be asked by one regulator to provide more detailed information about an incident and then that could be subsequently used against you in some sort of regulatory action," Camillo told Law360.

Regulatory fines and penalties including government investigations relating to a cyber incident are typically covered by cyber policies, but "the policy language can vary drastically from one policy to the next," Carter said, making it important that companies review their policies in light of the act and proposed rule.

Besides cyber policies, policyholders should take another look at their directors and officers policies, which could be implicated in certain actions arising from disclosures of a cyber event — for example, in a case where an announcement results in a significant drop in share prices of a company, leading to a shareholder suit.

"You'd want to make sure your D&O policy doesn't have a carve-out for cyber-related incidents or issues," Garrison of Honigman told Law360.

The act and proposed rule are indicative of the federal government's desire to better understand cyber threats and strengthen cybersecurity, but such actions also need to balance risks to the companies required to make disclosures, Camillo told Law360.

"We all need to collaborate in the best interest, but how do we sort of navigate this sort of the legal pitfalls that we've seen?" Camillo said.

The SEC "may not have fully appreciated the risks of litigation with the cybersecurity risks that the proposed rules have created," Shardul Desai, a cybersecurity and data privacy partner with Holland & Knight LLP, told Law360.

"Agencies need to think carefully about the impact that their proposed laws will have, the secondary or tertiary consequences that it will create, instead of trying to just address the immediate issue," Desai said.

--Additional reporting by Allison Grande and Tom Zanki. Editing by Tim Ruel.
