Harvard Law School Forum on Corporate Governance

SEC Proposes Unprecedented Cybersecurity Rules and Reporting Requirements

Posted by Adam Fee, Antonia M. Apps, and George S. Canellos, Milbank LLP, on Sunday, April 3, 2022

Editor's note: Adam Fee, Antonia M. Apps, and George S. Canellos are partners at Milbank LLP. This post is based on their Milbank memorandum.

On March 9, 2022, the SEC voted to propose rules mandating sweeping cybersecurity measures for public companies and foreign private issuers.[1] Most notably, the rules would impose a 4-day reporting requirement for domestic issuers who have experienced a "material cybersecurity incident." The rules would also require foreign issuers to disclose information about material cybersecurity incidents on Forms 6-K and 20-F.

The proposed rules broadly define a "cybersecurity incident" to cover effectively any intrusion of a company's systems: "an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein." Within four days of determining that such an incident is material—with no extension of time for an "ongoing investigation"—the issuer would have to disclose on an amended Form 8-K:

- when the incident was discovered;
- whether it was ongoing;
- a brief description of its nature and scope;
- whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
- the effect of the incident on operations; and
- whether the company "has remediated or is currently remediating the incident."

The proposed rules do not offer any further color on what may render a cybersecurity incident "material" but reiterate the conventional standard: "information is material if 'there is a substantial likelihood that a reasonable shareholder would consider it important.'"

For foreign issuers, the proposed rules would amend Form 6-K to add "cybersecurity incidents" as a reporting topic; and would add a new item to Form 20-F requiring companies to provide updates on previously disclosed cybersecurity incidents as well as to disclose when a "series of previously undisclosed individually immaterial" incidents have "become material in the aggregate."

[1] The SEC simultaneously published the Proposed Rules, along with a fact sheet and press release.

The proposed rules would also require significantly more detailed disclosures about all registrants' cybersecurity governance structure and processes, including descriptions of a company's procedures for identifying and managing cybersecurity threats as well as disclosure of the board's and management's roles and expertise in "assessing and managing cybersecurity" risk.

If implemented, these rules would dramatically alter the disclosure landscape for domestic and foreign issuers. For example, domestic issuers would be required to disclose, within four days of determining an incident was material, whether any data was stolen or accessed by attackers. In many instances, it will simply not be possible to make any reliable judgment about that sort of information within that period of time, which means that companies may often be in the position of disclosing a material incident where a number of important details remain uncertain or undetermined. Similarly, foreign issuers will be compelled to disclose incidents that had no plausible impact on US persons and may not have been subject to disclosure in the issuer's home country.

While most public companies have spent years, if not decades, building their internal cybersecurity monitoring and reporting systems, these proposed rules will put them to the test by requiring quick disclosure of cyber breaches, and expanding the scope of information in public filings that may be the subject of civil litigation and regulatory enforcement in the wake of such a breach. The proposed rules will now enter a public comment period, which will be the longer of either 60 days from March 9, 2022, or 30 days after publication of the proposal in the Federal Register.