CARLTON FIELDS

Four Takeaways From the SEC's Proposed Cyber Rule for Public Companies

March 11, 2022

What Happened?
On March 9, the Securities and Exchange Commission (SEC) published a proposed rule, File No. S7-09-22, that would significantly impact public companies' cybersecurity reporting obligations. Among other things, the rule would require:

- Reporting through Form 8-K **within four business days** of the company's determination that it has experienced a **"material cybersecurity incident."**
- **Standardized and periodic disclosures** on Form 10-K or, where applicable, Form 10-Q, of, among other things:
  - Cybersecurity policies and procedures;
  - Management's role in implementing those policies and procedures;
  - Board of directors' cybersecurity expertise, if any;
  - Updates regarding previously reported material cybersecurity incidents; and
  - Previously undisclosed immaterial cybersecurity incidents if they become material in the aggregate.

The SEC is receiving comments through early May 2022.

Four Takeaways for Publicly Traded Companies

These are significant proposed changes, which place the SEC's determination of the proper timing and content of an incident disclosure well ahead of what most states' laws currently require. Four of our top takeaways are as follows:

1. Given the short, four-business-day reporting obligation for material cybersecurity incidents, a company must prepare now for prompt detection, investigation, and response to those incidents. This preparatory work should include:
    1. Solidifying data maps (i.e., where is the company's data);
    2. Drafting, revising, and testing incident response plans;
    3. Developing relationships with key third parties, including law enforcement, forensics, and counsel; and
    4. Identifying outside counsel and media relations personnel to assist in drafting the Form 8-K disclosure and responding to what is often near-immediate investor, regulator, and other third party inquiry.
2. In light of the focus on disclosures related to board oversight and experience, companies should review their board composition to include one or more members familiar with cybersecurity issues. Board meetings should include cybersecurity as a standing agenda item with presentations from management and outside experts as needed. For financial services companies that are already subject to Title 23, Part 500 of the New York state regime, much of this will be familiar.
3. With the SEC compelling additional transparency regarding cybersecurity risks, events, and oversight, companies with existing, robust cybersecurity programs may enjoy a competitive advantage over their peers that do not have such programs. Management of such companies may also want to revisit retention and succession planning for their key cyber leaders, because this rule, if adopted, would lead to even tighter competition for cyber talent among public companies.
4. The SEC's focus on cybersecurity portends continued enforcement risk for public companies and regulated entities. Further, the rule and its disclosure obligations may increase class action litigation risk for public companies. This is a subject we have reported on in our firm's recent *Class Action Survey*.

We will monitor developments in connection with the proposed rule and provide further updates.

Authored By

John E. Clabby

Patricia M. Carreiro

Related Practices

Cybersecurity and Privacy
Securities Litigation and Enforcement
Securities Transactions and Compliance
SEC Enforcement

Related Industries

Securities & Investment Companies