Blogs
July 27, 2023
The SEC Adopts New Cybersecurity Risk Disclosure Rules!

Yesterday, the SEC **adopted** new cybersecurity risk disclosure rules – here's the **186-page adopting release** and here's the **fact sheet**. Here are seven things to know:

1. **New Form 8-K Item 1.05** – A new Item 1.05 for Form 8-K requires companies to disclose any cybersecurity incident they determine to be material and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations. This disclosure mainly focuses on the impacts of a cybersecurity incident, not so much on the details of the incident itself. Companies aren't required to disclose whether data has been compromised, the remediation status of an incident or system vulnerabilities in the kind of detail that could impair a company's attempt to remediate.

   The Form 8-K must be filed within four business days of the company determining the cybersecurity incident is material. Any updates on a particular incident disclosed on a Form 8-K should be made on an amendment to that 8-K.

2. **Safe Harbor for Form S-3 Eligibility** - As expected, Form S-3 has been updated to add Item 1.05 to the safe harbor list of Form 8-K items for which an untimely filing will not jeopardize S-3 eligibility.

3. **Assess Materiality Without "Unreasonable Delay" -** Companies must make their materiality determination without unreasonable delay following discovery of an incident. Pages 37-38 of the adopting release provide some color on what may – or may not – be an "unreasonable delay." Here is an excerpt from those pages:

   "If the materiality determination is to be made by a board committee, intentionally deferring the committee's meeting on the materiality determination past the normal time it takes to convene its members would constitute unreasonable delay.

As another example, if a company were to revise existing incident response policies and procedures in order to support a delayed materiality determination for or delayed disclosure of an ongoing cybersecurity event, such as by extending the incident severity assessment deadlines, changing the criteria that would require reporting an incident to management or committees with responsibility for public disclosures, or introducing other steps to delay the determination or disclosure, that would constitute unreasonable delay."

4. **Limited Disclosure Exceptions** – One significant change to the final rule, as compared with the proposal, was the addition of limited exceptions to the Form 8-K disclosure requirement. There is a narrow, time-limited, exception if the US Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing. Page 35 of the adopting release provides this gloss on this process:

"We have consulted with the Department of Justice to establish an interagency communication process to allow for the Attorney General's determination to be communicated to the Commission in a timely manner. The Department of Justice will notify the affected registrant that communication to the Commission has been made, so that the registrant may delay filing its Form 8-K."

There is also a limited exception for telecommunications carriers that are required under 47 CFR § 64.2011 to delay disclosure of certain incidents in connection with notification to the US Secret Service and FBI.

5. **Form 10-K Disclosure for Cybersecurity Risk Management and Strategy** - New Regulation S-K Item 106 requires companies to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company.

As noted in new Item 106(a) of Regulation S-K, "cybersecurity incident" means an unauthorized occurrence, or a series of related unauthorized occurrences, 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 – and "cybersecurity threat" means any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

6. **Form 10-K Disclosure for Cybersecurity Governance** - Item 106 requires companies to describe the board's risk oversight from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats. The proposed requirement for proxy statement disclosure regarding cybersecurity expertise on the board was dropped in the final rule in response to comments.

7. **Compliance Dates** - The rules become effective 30 days from when they are published in the Federal Register. And compliance takes effect as follows:

- **Form 8-K Item 1.05** - All companies other than smaller reporting companies must begin complying on the later of 90 days after the date of publication in the Federal Register or December 18, 2023. Smaller reporting companies will have an additional 180 days and must begin complying on the later of 270 days from the effective date of the rules or June 15, 2024.

- **Form 10-K** - All companies must provide such disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. So the compliance starts with calendar year fiscal year companies in their next Form 10-K.

- **iXBRL Tagging –** Inline XBRL tagging of data will be required beginning one year after the initial compliance dates described above.

Explore more in

Corporate Law