Lowenstein Sandler

Client Alert

Privacy & Cybersecurity

December 21, 2023

The SEC Cybersecurity Rules Are Now Effective: What You Need to Know and Do Now

By Mary J. Hildebrand CIPP/US/E, Daniel C. Porco, and Judith G. Rubin CIPP/US/E, CIPT

The Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (the "Cybersecurity Rules"), which the Securities and Exchange Commission (SEC) had adopted earlier this year, became effective on December 18. The Cybersecurity Rules codify the obligation of public companies to report material cybersecurity incidents and mandate the disclosure of cybersecurity governance practices and associated risks. Previously, reporting obligations allowed companies greater discretion, especially when determining whether a cybersecurity incident was "material" to the business.

Media headlines tend to obscure the material changes that Boards of Directors, Chief Information Security Officers (CISOs), and executive management teams may need to make in order to ensure compliance. It is currently unknown precisely what level of detail or documentation will satisfy the SEC that a registrant has complied with the Cybersecurity Rules. Nonetheless, it's abundantly clear that the Boards of Directors and executive management personnel of public companies will be held accountable, so careful preparation is critical.

What Companies Are Subject to the Cybersecurity Rules, and When?

The Cybersecurity Rules apply to corporations, limited liability companies, and partnerships that are subject to the regulations and disclosure requirements of the Securities Exchange Act of 1934, and to business development companies subject to the Investment Company Act of 1940 (collectively, "registrants" or "public companies"). Because registrants frequently rely on third-party service providers that are also at risk for cyberattacks, the Cybersecurity Rules state explicitly that a cyberattack at any service provider may have a material impact on registrants.

All registrants must disclose detailed information regarding cybersecurity governance and risk factors in annual reports starting with fiscal years ending on or after December 15, 2023, and comply with incident disclosure requirements beginning December 18, 2023 (smaller reporting companies have until June 15, 2024).

What Do the Cybersecurity Rules Require?

Disclosure of Cybersecurity Governance and Cybersecurity Risk Factors in Annual Reports. Registrants must disclose their internal cybersecurity governance practices, including detailed descriptions of the following:

- Processes used by the Board of Directors to oversee cybersecurity risks, such as appointment of board committees and standardized reporting on cybersecurity risks to the Board and/or appropriate Board committee.
- Management's role in assessing and managing material risks from cybersecurity threats, including designation of specific positions such as CISOs and/or committees and their relevant expertise (e.g., prior work experience in cybersecurity, relevant degrees or certifications, or other knowledge, skills, or background in cybersecurity); the processes used to stay informed of cybersecurity incidents and monitor their prevention, detection, mitigation, and remediation; and reporting obligations to the Board of Directors and/or a Board committee.

Cybersecurity Risk Factors. Registrants are required to describe their processes (if any) for assessing, identifying, and managing material risks from cybersecurity threats. Further, registrants must undertake an assessment of whether any risks from cybersecurity threats, including risks from previous incidents, have materially affected them or are reasonably likely to materially affect them in the future. The assessments should be appropriately documented to accommodate any regulatory inquiries.

Disclosure of Material Cybersecurity Incidents. Registrants are obligated to disclose any cybersecurity incident determined to be material, including the material aspects of its nature, scope, timing, and impact (or reasonably likely material impact) on the registrant.

Because registrants frequently rely on third-party service providers that are also at risk for cyberattacks, the Cybersecurity Rules state explicitly that a cyberattack at any service provider may have a material impact on registrants. The SEC does not require registrants to disclose details that would interfere with their incident response or remediation efforts. As in other securities contexts, a determination of whether information is material must be made from the perspective of a reasonable investor, considering all relevant quantitative and qualitive facts and circumstances.

The timeline for disclosing material cybersecurity incidents is very tight:

- Registrants must determine if a cybersecurity incident is material "without unreasonable delay" after discovery of the incident.
- Material cybersecurity incidents must be disclosed (Form 8-K) no later than four business days after the determination of materiality.
- If relevant information is not yet available, registrants must include a statement to this effect and, within four business days after it becomes available, file an amendment that contains this information.

Registrants may request a delay in disclosure of cybersecurity incidents (i) if there is an active law enforcement investigation, or (ii) the U.S. Attorney General ("AG") decides that disclosure impacts national security or public safety and notifies the SEC in writing. Disclosure cannot be delayed more than 120 business days without an exemptive order from the SEC. The Federal Bureau of Investigation (FBI) released the DOJ Material Cybersecurity Incident Delay Determinations Guidelines and FBI Policy Notice, instructing victims how to request delays in disclosure for national security or public safety reasons. The FBI will not process delay requests unless they are received by immediately upon a registrant's determination that disclosure of a cybersecurity incident to the SEC is required.

What Should Registrants Do Now?

The Cybersecurity Rules require an enhanced level of public disclosure regarding cyber preparation and accountability for material cyber incidents that impacts all public companies regardless of size, industry, or prior commitments to cybersecurity. Recommended immediate next steps include:

Ensure that the registrant has appropriate cybersecurity policies and procedures in place, which are regularly tested and updated.

Any organization–even if it already has robust cybersecurity procedures–should revisit its cybersecurity framework in light of these new requirements and promptly remedy any gaps. Registrants that do not yet have internal processes to identify and mitigate cybersecurity risks (including incident response and business continuity plans) need to move expeditiously.

Prepare for when (not if) a cyber incident occurs.

As part of its incident response plan, a registrant should ensure that any incident is assessed for materiality without unreasonable delay and, if required, disclosed under the Cybersecurity Rules. Management should also consider

establishing the criteria it will use to determine whether an incident is material. While the constantly evolving nature of cyberattacks makes it unlikely that materiality can be determined in advance, having a preexisting structure provides guidance in a stressful situation and adds an element of objectivity to the analysis.

Monitor developments and adjust.

The SEC promulgated the Cybersecurity Rules to standardize reporting of cybersecurity incidents and enhance transparency regarding cybersecurity risk and mitigation strategies. The prevalence and increasing sophistication of cyberthreats virtually guarantee that the Cybersecurity Rules will be amended, practices will change, and enforcement strategies will be updated to meet new challenges. Leadership's obligation is to ensure compliance across the enterprise and maintain sufficient flexibility to adapt quickly as necessary.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Founder & Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com

DANIEL C. PORCO
Counsel
T: 646.414.6811
dporco@lowenstein.com

JUDITH G. RUBIN CIPP/US/E, CIPT
Counsel
T: 212.419.5908
jrubin@lowenstein.com