BRACEWELL

SEC Cybersecurity Reporting Requirements for Public Companies: Applying Old Standards to New Risks

Update

August 28, 2023 | 3 minute read

On July 26, 2023, the Securities and Exchange Commission ("SEC") issued a final rule that requires registrants to provide enhanced and standardized disclosures regarding "cybersecurity risk management, strategy, governance and incidents." This rule, the culmination of discussion following the March 9, 2022 proposed rule, applies to public companies that are subject to the Securities Exchange Act of 1934 and takes effect September 5, 2023.[1]

Corporate cybersecurity risk has increased dramatically in recent years, the result of the widespread—and still growing—use of digital technologies and AI, the new normal of hybrid work environments, the growth of crypto assets and the rise in illicit profits from ransomware and stolen data. That increased risk, and its associated costs, has prompted investor concerns over access to timely, consistent and understandable information related to cybersecurity.

In a press release, SEC Chair Gary Gensler explained the importance of the new requirements to investors: "[w]hether a company loses a factory in a fire – or millions of files in a cybersecurity incident – it may be material to investors."[2] Mr. Gensler acknowledged that "[c]urrently, many public companies provide cybersecurity disclosure to investors," but asserted that "companies and investors alike, however, would benefit if this disclosure were made in a more consistent, comparable, and decision-useful way."[3] The new rules seek to accomplish this in three significant ways, relying on the familiar legal concepts of reasonableness and materiality.

1. Form 8-K Material Cybersecurity Incident Reporting

Registrants must disclose, on the new Item 1.05 of Form 8-K, any material cybersecurity incident. The disclosure must include all material aspects of the incident including its nature, scope, timing, and material impact, or reasonably

Related People

Seth
Partner
NEW YORK
+1.212.508.6165
seth.ducharme@bracewell.com

Maggie "Meg" Beasley
Senior Counsel
NEW YORK
+1.212.508.6180
margaret.beasley@bracewell.com

Anissa
Associate
NEW YORK
+1.212.938.6403
anissa.adas@bracewell.com

Related Industries

Finance

Related Practices

Financial Institutions
Government Enforcement & Investigations
Cryptocurrency & Blockchain
Data Security & Privacy

likely material impact on the registrant. This disclosure must be made within four business days of the determination that an incident is "material."

2. Form 10-K Annual Disclosures

Registrants must describe, in S-K Item 106 on the Form 10-K, (a) any processes for assessing, identifying and managing material risks from cybersecurity threat; (b) the board of directors' oversight of cybersecurity threats and (c) management's role in assessing and managing material threats from cybersecurity threats.

3. Foreign Private Issuers

Foreign private issuers will be required to disclose information on material cybersecurity incidents in accordance with an amended Form 6-K and information regarding cybersecurity risk management, strategy, and governance on Form 20-F.

Definitions

While these requirements seem simple, the devil will be in the definitions. Registrants should pay close attention to how the Commission defines key terms in the new rule to ensure full compliance.

- *Cybersecurity incident*: 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.
- *Cybersecurity threat*: 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.
- *Materiality*: Significantly, the SEC did not define "materiality" in the new rules, explaining that "[c]arving out a cybersecurity-specific materiality definition would mark a significant departure from current practice and would not be consistent with the intent of the final rules."[4] Instead, the SEC offered the following guidance: "consistent with the standard set out in the cases addressing materiality in the securities laws, that information is material **if there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the total mix of information made available**.[5]"

Changes from the Proposed Rule

The Final Rule incorporates several key changes from the proposed rule, providing insight into the Commission's enforcement priorities. These include the following:

- Narrowing the scope of the cyber incident disclosures and adding a limited delay for disclosures that would pose a substantial risk to national security or public safety.
- Omitting the aggregation of immaterial incidents for disclosure in Forms 10-Q and 10-K; however, a series of related unauthorized occurrences may prompt a requirement to provide disclosures on Form 8-K.
- Streamlining the proposed disclosure elements related to risk management, strategy and governance with a focus on processes as opposed to specific policies and procedures.
- Removing the proposed requirement to disclose cybersecurity expertise of the board.
- Adding transition provisions for disclosing material cyber incidents on Form 8-K and for providing annual cybersecurity risk management, strategy and governance disclosures.

---

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216, U.S. Securities and Exchange Commission (July 26, 2023). The Form 10-K and Form 20-F disclosures will be due beginning with annual reports for fiscal years ending on or after December 15, 2023. The Form 8-K and Form 6-K disclosures will be due beginning 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 before they must begin providing the Form 8-K disclosure.

[2] SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, U.S. Securities and Exchange Commission, (July 26, 2023).

[3] *Id*.

[4] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216, U.S. Securities and Exchange Commission (July 26, 2023) at 80.

[5] *Id*.