In brief

SEC adopts cybersecurity disclosure rules

No. US2023-05
July 26, 2023
(updated August 10, 2023)

> Increasingly, cybersecurity risks and incidents are a fact of modern life. When material incidents occur, they can have a range of consequences—including financial, operational, legal, or reputational.
>
> SEC Chairman Gensler, July 26, 2023

At a glance

The SEC has adopted amendments that require enhanced and standardized disclosures related to cybersecurity for public companies, including foreign private issuers.

What happened?

On July 26, the SEC adopted amendments intended to enhance and standardize disclosures related to cybersecurity. The amendments require timely disclosure of material cybersecurity incidents and annual disclosures related to cybersecurity risk management, strategy, and governance. The final rules apply to all registrants reporting under the 1934 Exchange Act, with comparable requirements for foreign private issuers (FPIs). The final rules reflect several changes to elements described in the 2022 proposal, including streamlined disclosures and some additional clarity about the aggregation and reporting of individually immaterial cybersecurity incidents.

Timely disclosure of material incidents

A US domestic registrant or an FPI filing on domestic forms will be required to report a material cybersecurity incident on new Item 1.05 of Form 8-K within four business days after the registrant determines that the incident is material. The rule provides for a series of extensions if the US Attorney General notifies the SEC in writing that immediate disclosure would pose a substantial risk to national security or public safety.

The SEC has defined a cybersecurity incident to mean "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." The determination of whether an incident is material will be based on the definition of materiality used in the federal securities laws. Registrants must determine the materiality of an incident without unreasonable delay following discovery.

The definition of an incident includes a series of related occurrences. Events may be related if they involve, for example, the same malicious actor or exploitation of the same vulnerability. When a company concludes that it is materially affected by a series of related unauthorized occurrences, the Form 8-K requirements will apply, even if each individual occurrence is determined to be immaterial.

The Form 8-K is required to describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations. A registrant need not disclose specific or technical information about its planned response to the

incident, or its systems, in such detail as would impede its response or remediation of the incident.

If information required to be disclosed in the Form 8-K is not determined or not available at the time of the required filing, the registrant should include a statement to this effect in the filing. Within four business days of when this information is determined or becomes available, the registrant must file an amendment to its Form 8-K.

FPIs filing on FPI forms would be required to furnish information regarding material cyber incidents on a Form 6-K, assuming the other criteria outlined in the instructions to Form 6-K are met.

Annual disclosures of risk management, strategy, and governance

New Item 106 in Regulation S-K will require registrants to provide information about their cybersecurity risk management, strategy, and governance in their annual report on Form 10-K or Form 20-F.

Risk management and strategy

Registrants are required to describe the processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. Required disclosures include the following (non-exclusive) items:

- Whether and how any such processes have been integrated into the registrant's overall risk management system or processes
- Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes
- Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider

The registrant must also describe whether and how 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 registrant, including its business strategy, results of operations, or financial condition.

Governance

Disclosure is required about management's and the board of directors' oversight of cybersecurity risk, including:

- A description of the board of directors' oversight of risks from cybersecurity threats
  - The identity of any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats
  - The processes by which the board or such committee is informed about such risks

- A description of management's role in assessing and managing the registrant's material risks from cybersecurity threats, including the following (non-exclusive) disclosure items:
  - Whether and which management committees or positions are responsible for assessing and managing such risks, and the relevant expertise of such persons or members
  - The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents
  - Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Why is this important?

The new rules significantly expand registrants' annual disclosures, providing investors and other stakeholders with more standardized information about a registrant's cybersecurity risk management, strategy, and governance. The disclosures of material cybersecurity incidents will require more specific details and may occur sooner than registrants have historically reported such events, requiring changes to systems, processes, and controls.

What's next?

Registrants must begin complying with the requirement to report a material cybersecurity incident, as defined, on Form 8-K or Form 6-K on December 18, 2023. Smaller Reporting Companies will have until June 15, 2024.

All registrants are required to comply with the annual disclosure requirements beginning with annual reports for fiscal years ending on or after December 15, 2023.

To have a deeper discussion, contact:

Mary Grace Davenport
Partner
Email: mary.grace.davenport@pwc.com

Ryan Spencer
Partner
Email: ryan.spencer@pwc.com

Matt Horowitz
Director
Email: matt.horowitz@pwc.com

Lauren Buoniconti
Director
Email: lauren.buoniconti@pwc.com

For more PwC accounting and reporting content, visit us at viewpoint.pwc.com. On the go? Take our podcast series with you at the Viewpoint podcasts page.