# SEC ADOPTS NEW RULE REGULATING CYBERSECURITY DISCLOSURES

14 AUGUST 2023 • ARTICLE

**The new Securities and Exchange Commission ("SEC") rules mandate for U.S. public companies (i) through Form 8-K, the reporting by a U.S. public company of material cybersecurity incidents within four business days of the company's determination of materiality; and (ii) through Form 10-K, annual disclosures by a U.S. public company detailing the company's cybersecurity risk management, strategy, threat management processes, and cybersecurity governance.**

> "A public company must disclose the nature, scope and timing of an incident, along with the incident's reasonably likely material impact on the company, the company's financial condition and its results of operations."

Foreign private issuers have comparable annual disclosures in Form 20-F annual reports and reports of material cybersecurity incidents may be addressed through Form 6-K.

## REQUIREMENT

The SEC finalized its rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, requiring that public companies, including foreign private issuers, promptly disclose material cybersecurity incidents and annually disclose certain information about cybersecurity. Specifically, the new rule—adopted on July 26, 2023 and effective on September 5, 2023—requires each public company, including a foreign private issuer, to describe in its annual report:

- the processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats;
- whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect the company's business strategy, results of operations, or financial condition;
- the board's oversight of risks from cybersecurity threats; and
- management's role in assessing and managing material risks from cybersecurity threats.

In addition, a public company that reports on U.S. domestic SEC forms (i.e., a company that files Form 8-Ks, 10-Qs, and 10-Ks) ("U.S. public company") must report a "cybersecurity incident" within four business days of its determination that the incident experienced by such company is "material." The SEC clarified that determining materiality contemplates both qualitative and quantitative factors, a standard consistent with precedent securities law. Designed to improve investor understanding of cybersecurity risks faced by public companies and following an increase in cybersecurity threats, the new rule aims to provide additional information to investors and potential investors to assist them in making their investment decisions.

## WHAT ARE COMPANIES REQUIRED TO DISCLOSE AFTER A MATERIAL CYBERSECURITY INCIDENT?

### U.S. public companies

New Item 106(b) of Regulation S-K requires disclosure by a U.S. public company of (i) processes for assessing, identifying, and managing material cybersecurity risks, (ii) whether those processes have been unified into the company's broader risk management system, (iii) whether the company engages with third parties to assist with the risk management procedures and (iv) whether the company has processes to recognize material cybersecurity threats linked to its use of any third party service provider. A U.S. public company must also disclose whether and how these cybersecurity threats may be likely to materially affect the company's business, financial condition and results of operations.

The new Regulation S-K Item 106(c) requires a U.S. public company to disclose information related to the cybersecurity governance of the company. Registrants must describe the board's oversight of risks from cybersecurity threats and describe management's role in assessing and managing material risks from cybersecurity threats. The new regulations require disclosure of the board's cybersecurity risk management role, and specifically:

"The new Regulation S-K Item 106(c) requires a U.S. public company to disclose information related to the cybersecurity governance of the company."

- whether the entire board, specific members of the board, or a committee of the board is responsible for cybersecurity oversight;
- the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and
- whether and how the board, board members, or committee considers cybersecurity risks as part of its business strategy, risk management and financial oversight.

### Foreign private issuers

Foreign private issuers will now largely be required to disclose material cybersecurity incidents and provide general annual disclosures in a similar way that domestic issuers are required. Specifically, the new rule amended Form 20-F to include requirements parallel to Item 106 regarding a foreign private issuer's governance, strategy, and risk management. Likewise, the Form 6-K used by foreign private issuers will also be amended to include reference to disclosure of material cybersecurity incidents. A foreign private issuer will need to disclose information about material cybersecurity incidents that it discloses or otherwise publicizes in a foreign jurisdiction, to any stock exchange, or to security holders, and the SEC has added "material cybersecurity incidents" to the items that may trigger a current report on Form 6-K.

This article was written by Partner Steven Hollander and Associate Krisly Zamor. If anyone needs assistance determining the appropriate disclosures related to cybersecurity incidents, or determining proper risk management, strategy, and governance disclosure, please contact one of the authors or your regular Watson Farley & Williams contact.

## KEY CONTACTS


**STEVEN HOLLANDER**
PARTNER • NEW YORK

T: +1 212 922 2252

shollander@wfw.com

**FILANA R. SILBERBERG**
PARTNER • NEW YORK

T: +1 212 922 2225

fsilberberg@wfw.com

**MICHAEL SMITH**
PARTNER • NEW YORK

T: +1 212 922 2204

msmith@wfw.com

**WILL VOGEL**
PARTNER • NEW YORK

T: +1 212 922 2280

wvogel@wfw.com

**KRISLY ZAMOR**
ASSOCIATE • NEW YORK

T: +1 212 922 2203

KZamor@wfw.com

This publication constitutes attorney advertising.