ECKERT SEAMANS
ATTORNEYS AT LAW

June 27, 2023

Cybersecurity, Data Protection & Privacy Update

Proposed SEC Cybersecurity Risk Governance Rules for Public Companies

By Matthew H. Meade and Elizabeth Wilson

WHAT HAPPENED

The U.S. Securities and Exchange Commission ("SEC") developed proposed Rules for publicly traded companies that are intended to "enhance and standardize" disclosures regarding a company's cybersecurity compliance program and cybersecurity incident reporting.

It is anticipated that the SEC will finalize these rules in **October 2023**.

WHO DOES THIS AFFECT

All publicly traded companies that are subject to mandatory reporting under the Securities Exchange Act of 1934.

HOW THIS AFFECTS YOU

Publicly traded companies will need to provide the following cybersecurity disclosures as described in the table below.

Table 1: Proposed SEC Cybersecurity Disclosure Requirements

Cybersecurity Incident Reporting	Must disclose: • "material" cybersecurity incidents; • current information on previously disclosed incidents; and • instances where a series of previously undisclosed immaterial cybersecurity incidents is considered "material" in the aggregate. Table 2 below provides further information on the proposed SEC cybersecurity incident reporting requirements.
Cybersecurity Policies and Procedures	Must disclose: • the company's policies and procedures to identify and manage cybersecurity risk; and • whether the company considers cybersecurity risks as part of its business strategy, financial planning, and capital allocation.
Board Requirements	Must describe the board's: • oversight of the company's cybersecurity risk; and • cybersecurity expertise and the nature of such expertise.
Senior Management Requirements	Must describe senior management's: • cybersecurity expertise; • role in assessing and managing cyber risks; and • role in implementing its cyber policies, procedures, and strategies.

The SEC proposed rules describe when a public company should report a cybersecurity incident and what information should be provided in the disclosure. Please see Table 2 below for further information.

Table 2: Material Cybersecurity Incident Reporting Requirements

Materiality Trigger	"Material" means 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. The company would need to consider, from the viewpoint of an investor, all relevant facts and circumstances surrounding the cybersecurity incident.
Notification Period	The company must disclose the cybersecurity event in a current report on Form 8-K within four business days of becoming aware that the incident is "material." The materiality determination must be made "as soon as reasonably practicable after discovery of the incident" and should not be delayed due to ongoing internal or external investigations into the incident. Delayed notifications under state data breach laws due to an ongoing law enforcement investigation may not be used to delay SEC disclosures.
Required Information to Disclose	Companies will need to disclose: (i) when the company discovered the incident and whether it is ongoing; (ii) a brief description of the nature and scope of the incident; (iii) whether any data was stolen, altered, accessed, by an unauthorized party or used by for any other unauthorized purpose; (iv) the effect of the incident on the company's operations; and (v) whether the company has remediated or is currently remediating the incident. It is not necessary to disclose specific technical information about the company's security systems, system vulnerabilities, or response to the incident to the extent it would hinder the company's response and/or remediation of the incident.

ACTIONS YOU SHOULD TAKE

To prepare for these new disclosure requirements, public companies should:

- review their cybersecurity policies and procedures to cover the new disclosure requirements;
- review and update its data breach response plan to ensure that it can accommodate a four-day SEC reporting requirement as well as other state breach notification laws reporting timeframes;
- ensure senior and board level leadership has sufficient involvement and oversight over assessing the company's cyber risk level and implementing the company's cyber program; and
- fill senior and board level leadership roles with individuals having cybersecurity experience, to the extent possible, or provide its leadership with adequate cyber training opportunities.

ECKERT SEAMANS ATTORNEYS AT LAW

This Legal Update is intended to keep readers current on developments in the law. It is not intended to be legal advice. If you have any questions, please contact Matthew Meade at 412.566.6983 or mmeade@eckertseamans.com, Elizabeth Wilson at 215.851.8497 or ewilson@eckertseamans.com, or any other attorney at Eckert Seamans with whom you have been working.