Alert

COZEN O'CONNOR

SEC Proposes New Rules for Cybersecurity Incident Reporting

March 28, 2022

On March 9, 2022, the U.S. Securities and Exchange Commission (SEC) proposed new rules that would require public companies to report detailed information about material cybersecurity incidents affecting their business and their cybersecurity risk management and governance. The new requirements are intended to expand cybersecurity incident reporting and promote increased cybersecurity risk management and governance among publicly traded companies in the United States.

Form 8-K Changes

The SEC proposes to require publicly traded companies to report, via Form 8-K, material cybersecurity incidents within four business days after a determination that an incident has occurred. The disclosure timeline starts, not at the point of the initial discovery of the incident, but when a determination of materiality is made. Therefore, companies will not be penalized for late reporting if an incident initially appeared minor but was later determined to be significant enough to trigger the reporting requirement. The initial SEC proposal does not allow companies to delay reporting if law enforcement is investigating and requests a delay in public disclosure of the incident. The standard proposed by the SEC for determining materiality is consistent with the standard articulated by the Supreme Court: an incident is material if "there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision."

The proposed rule includes a non-exhaustive list of examples of cybersecurity incidents that might trigger the reporting requirement:

1. an unauthorized incident that compromises the confidentiality, integrity, or availability of data, a system, or a network, or violates the company's security policies or procedures;
2. an unauthorized incident that causes degradation, interruption, loss of control, damage to, or loss of operational technology systems;
3. an incident in which an unauthorized party accesses (or a party exceeds authorized access) and alters, or has stolen, sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the company;
4. an incident in which a malicious actor offers to sell or threatens to publicly disclose sensitive company data; or
5. an incident in which a malicious actor demands payment to restore company data that was stolen or altered.

Forms 10-Q and 10-K Changes

Additionally, the SEC would require material updates to previously reported cybersecurity incidents. Updates would be included in the company's Form 10-Q or Form 10-K for the period in which the update occurred. Non-exhaustive examples of updates include any material impact or potential material impact of the incident on the company's operations or financial condition, whether the company has remediated the incident, and any changes in the company's policies and procedures resulting from the cybersecurity incident and how the incident may have informed such changes.

The SEC also proposes to require disclosure in Form 10-Q or Form 10-K when a series of

Christopher Dodson

Member

cdodson@cozen.com
Phone: (215) 665-2174
Fax: (215) 372-2408

Andrew Baer

Chair, Technology, Privacy & Data Security

abaer@cozen.com
Phone: (215) 665-2185
Fax: (215) 372-2400

Related Practice Areas

- Capital Markets & Securities
- Corporate
- Corporate Governance
- COSECURE

previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate. For example, if one malicious actor engages in a number of smaller but continuous cyber-attacks related in time and methods against a company and, collectively, they are either quantitatively or qualitatively material.

If incidents become material in the aggregate, companies would need to disclose:

1. when the incidents were discovered and whether they are ongoing;
2. a brief description of the nature and scope of the incidents;
3. whether any data was stolen or modified;
4. the impact of the incidents on the company's operations; and
5. whether the company has remediated or is currently remediating the incidents.

Risk Management and Strategy Disclosures in Form 10-K

The SEC proposes to amend Form 10-K further to require disclosures about a company's cybersecurity risk management systems, including its policies and procedures for identifying, assessing, and managing the risks. The SEC would require the disclosure, as applicable, of whether:

1. the company has a cybersecurity risk assessment program;
2. the company engages third parties to assess its cybersecurity risk program;
3. the company has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider;
4. the company undertakes activities to prevent, detect, and minimize the effects of cybersecurity incidents;
5. the company has business continuity, contingency, and recovery plans in the event of a cybersecurity incident;
6. previous cybersecurity incidents have informed changes in the company's governance, policies, and procedures or technologies;
7. cybersecurity-related risk and incidents have affected or are reasonably likely to affect the company's results of operations or financial condition; or
8. cybersecurity risks are considered part of the company's business strategy, financial planning, and capital allocation.

Governance Disclosures in Form 10-K

The proposed rule requires a description in a company's Form 10-K of the board's oversight of cybersecurity risk, management's role in assessing and managing cybersecurity risks, the relevant expertise of management, and its role in implementing the registrant's cybersecurity policies, procedures, and strategies. Examples of disclosures about the board's or management's respective roles include:

1. whether the entire board, specific board members, or a board committee is responsible for the oversight of cybersecurity risks;
2. the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic;
3. how the board or a board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight;
4. whether certain management positions or committees are responsible for measuring and managing cybersecurity risk;
5. whether the company has a designated chief information security officer;
6. the processes by which the responsible persons are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents; and
7. whether and how frequently such persons report to the board or a committee of the board about cybersecurity risk.

Board Cybersecurity Expertise Disclosures in Form 10-K

Finally, the SEC proposes to require a description of the cybersecurity expertise of the company's board. Examples include:

1. whether a director has prior work experience in cybersecurity, such as prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner;
2. whether a director has obtained a certification or degree in cybersecurity; and
3. whether a director has knowledge, skills, or other cybersecurity background, such as security policy and governance, risk management, security assessment, control evaluation, security architecture, and engineering, security operations, incident handling, or business continuity planning.

The proposed rules now enter a public comment period that will remain open until May 8, 2022 (60 days following publication of the proposing release on the SEC's website), or 30 days following publication of the proposing release in the Federal Register, whichever period is longer.