POLSINELLI | What a law firm should be.™

The SEC Raises the Stakes: New Cybersecurity Rules for Publicly Traded Companies Hit the Books in 2023

Overview

In 2023, the U.S. Securities and Exchange Commission ("SEC") issued its now-fully implemented Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule. The Rule reflects the reality that cybersecurity is now a major operational issue for companies and seeks to standardize the disclosures of cyber incidents and overall cyber risk management for publicly traded companies. It also marks a significant expansion of what information about their cybersecurity posture those companies must make public through their annual disclosures as well as in one-off 8-K disclosures in the event of a data security incident.

The Rule creates a few major requirements:

- *Disclosure of a Registrant's Risk Management, Strategy and Governance Regarding Cybersecurity Risks:* Companies must proactively include information about their processes for assessing, identifying and managing material risks from cybersecurity threats in their annual disclosures. Additionally, companies need to disclose if risks from cybersecurity threats, including those stemming from previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company. These disclosures must be made in a way that reasonable investors can understand, with the idea being that investors are increasingly factoring in a company's cybersecurity posture when deciding whether to invest in that company.
- *Disclosure Regarding the Board of Directors' Cybersecurity Expertise:* Companies must also describe management's role in assessing and managing material risks from cybersecurity threats, as well as the Board of Directors' oversight of these issues. This latter disclosure should identify the management positions responsible for assessing and managing the risks; the relevant expertise of the individuals in those positions; the processes by which management is informed about and monitors the prevention, detection, mitigation and remediation of cybersecurity incidents; and the threshold for management to escalate cyber risks to the Board or Board Committee. The purpose behind this separate disclosure is to give investors insight into not just a company's technical cybersecurity posture but also how much the senior levels of the company are factoring cybersecurity in their management decisions.

- *Timely Disclosure of Cybersecurity Incidents: C*ompanies must disclose cybersecurity incidents (usually in a Form 8-K filing) within four business days of determining they have experienced a "material" incident. The materiality of an incident must be determined "without unreasonable delay" and by considering factors such as the incident's impact on the company's reputation; customer or vendor relationships or competitiveness; and the possibility of litigation or regulatory investigations. In essence, materiality will be determined in a similar way as other 8-K filings – whether the incident could influence the investment decision of a reasonable shareholder. Once the materiality threshold is met, the disclosure must describe the nature, scope and timing of the incident, as well as the "material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations." The disclosure must also be amended as additional material information is discovered after the initial filing.
    - *Note:* The Rule has a built-in appeal process to delay this disclosure if the U.S. Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety. This process involves the Federal Bureau of Investigation ("FBI"), the Department of Justice ("DOJ") and the SEC, all of which have issued guidance on their portion of the process. Although time will tell, based on these guidance documents, it is likely that an exception is rarely going to be given.
    - *Another Note:* The SEC is not exempting companies from providing disclosures regarding cybersecurity incidents on third-party systems they use. Depending on the circumstances of an incident that occurs on a third-party system, disclosure may be required by both the service provider and the customer of those services, by one or the other, or by neither.
    - *A Final Note:* Threat actors are clearly aware of the SEC's expectation that incidents are reported quickly, as there have already been a few instances where the threat actors who attacked a company then subsequently reported the attack to the SEC after their victims failed to do so. This tactic is clearly aimed at putting additional pressure on the company as it navigates its response to the threat actor's attack.

How to Comply

In response to the new Rule, companies should review their overall cybersecurity posture, their cybersecurity management programs, and their incident response procedures. Specifically, companies subject to the Rule should focus on a few areas of work:

- *Enterprise-Wide Cybersecurity Strategy*

Gone are the days when IT could be siloed off and asked to "handle the technical stuff." Companies now need to have an in-depth cross-department strategy for handling cybersecurity. That strategy also needs to be regularly tested, evaluated and revised. This requires an organization with a cybersecurity governance structure that is empowered and held accountable at the highest levels of the organization, and which trickles down throughout the company.

- *Board Training*

With the Rule's requirement that organizations demonstrate their Board's proficiency and oversight of cybersecurity risks, the Board should get adequate reports and presentations on the general cyber threat landscape and what the organization is doing in response to that landscape.

- *Cyber Incident Response Planning and Testing*

By planning ahead and properly preparing for a cybersecurity incident, an organization can respond to an actual incident in a more efficient and strategic way. In doing so, it may be able to keep an incident from becoming material and therefore reportable. Companies need to assess and implement an enterprise-wide Incident Response Plan ("IRP"). A good IRP addresses how the entire organization will respond to an incident. Limiting an IRP to the IT and security team's role results in the organization not taking into account all of the business, legal and messaging decisions that need to be made during a cyber incident. Once an IRP is developed, it should be tested through regular tabletop exercises.

Additionally, executive leadership should think through the materiality standard for cyber incidents. While materiality is not a new concept for 8-K purposes, the short timelines imposed by the Rule mean that quickly making this determination in the midst of a data incident will be challenging. Companies need to think ahead to consider the current threat landscape and how particularly disruptive incidents, like ransomware, may impact the organization operationally, financially and reputationally.

- *Business Continuity Planning and Testing*

Ransomware is one of the most common types of cyberattacks and is the most disruptive to an organization. It is therefore the one most likely to create a material cyber incident. As a result, organizations need to implement and regularly test a business continuity plan and backup systems. This extends to plans for events involving third-party vendors.