LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

4 Ways Company Execs Can Prep For SEC Cybersecurity Rule

By **Jennie Wang VonCannon** (August 9, 2023, 5:07 PM EDT)


Jennie Wang VonCannon

With the release of its final rule on cybersecurity risk management, strategy, governance and incident disclosure on July 26, 2023, the U.S. Securities and Exchange Commission solidified one aspect of the cybersecurity rule that has been in the works for over a year.

This element requires public companies to make disclosures about material aspects of a cybersecurity incident — including a description of its nature, scope, timing and impact on the company — to their investors within four days of determining that such an incident is material.

When it proposed the cybersecurity rule in March 2022, the SEC waded into the mix of government regulations regarding cybersecurity for the first time, underscoring the government's increasing emphasis on companies' transparency and accountability for cyber incidents.

What materiality means in the context of the SEC's final cybersecurity rule will surely be litigated in the coming years, but the rule relies on the already-established standard of materiality set by the U.S. Supreme Court.

In TSC Industries v. Northway Inc. in 1976, the court ruled that a fact is material if there is "a substantial likelihood that the ... fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available."

Although a company cannot control when it will suffer a cybersecurity incident, it has more control over what information is in the total mix of facts made available to its investors about the company's cybersecurity program.

The determination of materiality of a cyber incident to a particular company and its shareholders is very fact-specific. This takes into account both the facts about the company itself, which can be determined now, in addition to facts about the particular cyber incident, which necessarily will be determined in the future.

General counsel, C-suite executives and other company leaders can undertake four factual assessments now to prepare their companies to respond quickly and agilely to the seemingly inevitable cyberattack in light of the new SEC cybersecurity disclosure requirements.

1. Conduct an assessment of the company's current cybersecurity regime.

Companies cannot make an assessment of what would be material to an investor without an understanding of the security controls they currently have in place to prevent cyberattacks and breaches.

Put simply, a company at the very least needs to know what data it possesses — from employee data to customer payment information to trade secrets, to name a few — where and in what form that data is stored, how the data is protected and, ideally, encrypted, and who is responsible for ensuring the data's security.

The depth and breadth of each company's cybersecurity program will vary, but conducting this assessment early and often — as the company's data needs and collections change over time — is crucial to be able to make a materiality determination.

2. Identify gaps and fill them.

As company leadership and information professionals dive into the details regarding their data and efforts to secure such data, to the extent gaps are identified, it will be important to address them without unreasonable delay.

Once a company is on notice about potential weaknesses in its cybersecurity protocols, how they are addressed will almost certainly be germane to any backward-looking assessment about the company's reasonableness in responding to a cyber incident — not to mention important to lowering the risk of a cyber incident in the first place.

3. Create or update the company's incident response plan.

Given the ubiquity of data breaches and cybersecurity incidents in today's data-driven interconnected world, having a plan in place for how to respond to such situations is a must for a company's ability to minimize operational disruption, regulatory scrutiny and litigation risk.

Once an incident response plan is put in place, it is also a good idea to test it out on a regular basis through tabletop exercises, in which a company goes through a simulated cyber incident to both practice the procedures set out in the plan and illuminate any areas that can be improved.

4. Consider educating stakeholders about the company's cybersecurity protocols.

The SEC's cybersecurity rule also requires public companies to describe annually in their Form 10-K their boards' oversight of risks arising from cybersecurity threats, as well as management's role in assessing and managing such material risks.

It follows, then, that this assumes there will be board oversight and management of a company's cybersecurity risks.

Given that companies must make disclosures about such facts on an annual basis, they should consider whether they want to do so earlier or more often, especially since this could affect what is in the total mix of information available to investors about the company's cybersecurity regime and therefore possibly affect what is determined to be material.

Conclusion

Once a company has made these four key assessments, a determination should be made regarding what facts, if any, should be disclosed to their stakeholders — and when — to add to the total mix of information available about the company's cybersecurity regime.

In broad strokes, the more robust a company's cybersecurity protocols are and the more transparent the company is with its shareholders about its cyber regime as a general matter, the less likely a given cyber incident will rise to the level of material, such that it must be disclosed per the SEC's now-final cybersecurity rule.

Given that the rule will go into effect 30 days after it is published in the Federal Register, it is important for company leadership to consider undertaking these assessments as soon as possible.

Four days is not a lot of time during a cyberattack to determine what happened, what the effect is on the company and its data, and how to respond to it — let alone what is material to an investor such that it must be disclosed.

The more a company can do now with respect to the facts it can control, the more it can focus on the facts that it cannot in the unfortunate event of a cybersecurity incident.

Jennie Wang VonCannon is a partner at Crowell & Moring LLP. She served for over eleven years as a federal prosecutor, most recently as the Deputy Chief of the Cyber and Intellectual Property Crimes Section of the National Security Division in the U.S. Attorney's Office for the Central District of California.