Press Coverage | October 19, 2023

The SEC's Cybersecurity Rules

RELATED PROFESSIONALS

Kim Phan

Kim Phan, a partner in Troutman Pepper's Privacy + Cyber Practice Group, was quoted in the October 19, 2023 *Communications of the ACM* article, "The SEC's Cybersecurity Rules."

According to Kim Phan, a partner with national law firm Troutman Pepper, a public company is not required to make cybersecurity disclosures within four business days of the discovery of a cyber incident, but within four business days of the date that the company determines that the cybersecurity incident is material.

The rule provides for a limited delay in the Form 8-K disclosure when it could pose a substantial risk to national security or public safety, says Phan. However, a company's ability to earn this relief requires the intervention of the U.S. Attorney General, she says.

Whether the cyber incident is material, and how to determine that, is essential to understanding when to disclose it.

According to Phan, in addressing materiality, the SEC cybersecurity rule adopted the long-accepted definition of "materiality" from the U.S. Supreme Court decision on *TSC Industries, Inc. v. Northway, Inc.* 426 U.S. 438 (1976).

Phan said something is material if there is 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.

While public companies have experience applying the *TSC v. Northway* materiality standard, many companies may be uncomfortable applying these standards to a cybersecurity incident, Phan says.

…

The SEC rule holds C-suites and boards accountable for cybersecurity. Boards of directors must exercise oversight of cybersecurity risks. "Boards have taken an increased role in overseeing a company's cybersecurity policies and programs. They are actively looking for board members experienced with cybersecurity matters as cybersecurity requirements have become more detailed and demanding and the threats have grown," says Phan.

…

According to Phan, the rule attempts to focus disclosures on the material effects of a cybersecurity incident, rather than requiring extensive details about the incident itself, which critics of the rule argued that malicious actors could

misuse.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber