Van Houten in Cybersecurity Dive: SEC's Cyber Disclosure Rules, Key Considerations for the Board, C-suite and Risk Managers

November 27, 2023 Greg Van Houten

PRACTICES Insurance Recovery, Capital Markets and Securities

Haynes Boone Associate Greg Van Houten authored an article in *Cybersecurity Dive* with two founding partners at Naxo, Chris Tarbell and Dave Franzel, on new cybersecurity disclosure rules implemented by the Securities and Exchange Commission.

Read an excerpt below:

The Securities and Exchange Commission's new cybersecurity disclosure rules take effect on Dec. 18 and starting then, public companies must disclose material cyber incidents within four business days of determining that an incident is "material."

Companies will also have to disclose, via their annual Form 10-K, information regarding their cybersecurity strategy, risk management and governance practices.

Given the public nature of those disclosures, the SEC's heightened focus on cyber enforcement actions, and the active shareholder litigation landscape with respect to cyber incidents, it is critical that company leadership takes steps now to decrease risk and to prepare for the implementation of the SEC's new rules.

What company officials need to worry about can change depending on what they oversee. Here are the central cyber considerations for the board, corporate offices and risk managers ahead of the new rules.

Considerations for board members

Elevate cyber to the board level

Boards should be well-informed about an organization's cyber risk posture. Regular updates centered around well-curated cyber dashboards are excellent ways to provide engaging and informative material.

Internal or third-party cybersecurity professionals should drive these updates and be capable of synthesizing complex technical concepts for non-technical board members.

Prioritize cyber experience when considering future board additions

Having individuals on the board capable of independently evaluating cyber risk will increase the quality of decision-making with respect to cybersecurity.

The SEC's new rules also require disclosure of board-level cybersecurity expertise, and a lack of board-level expertise could be scrutinized by the SEC and/or shareholders.

Comply with new disclosure rules

At a minimum, companies must disclose in their Form 10-Ks the "board's oversight of risks from

cybersecurity threats."

If applicable, they must also "identify any board committee or subcommittee responsible" for such oversight "and describe the processes by which the board or such committee is informed about such risks."

Considerations for corporate officers

Have a plan

Before a cyber incident is identified, know who needs to be called.

Who takes the lead in responding? Who are the law firms, forensic personnel, public relations, ransom negotiators and crisis management experts who may need to be brought in? How are critical decisions made and what are each person's responsibilities?

All of this and more must be clearly documented in an incident response plan.

Test the plan

It is critical that the first time you run through an incident response plan is not on a real incident. Tabletop exercises are one of the most common ways to test incident response plans and can also be a great way to increase awareness of the cyber threat landscape among corporate leadership.

Tabletop exercises typically involve a third party simulating an impactful incident and coaching management through the organization's incident response plan.

Iterate on the plan

Incident response plans must evolve with the cyber threat landscape, regulatory requirements and changes to corporate governance. It is important to update incident response plans on a regular basis as well as in response to incident post-mortems, new disclosure rules and major changes to organizational structure.

To read the full article in *Cybersecurity Dive*, click here.