Published on *The National Law Review* https://natlawreview.com

SEC Adopts Final Cybersecurity Risk Management and Incident Disclosure Regulations

Article By:

Glenn A. Brown

Shea Leitch

After much anticipation, the Securities and Exchange Commission (the "Commission") has adopted Regulations (the "Regulations") regarding public companies' obligations to include disclosure in annual reports on Form 10-K (Form 20-F for foreign issuers) regarding material cybersecurity risks, risk management and governance, and to file current reports on Form 8-K (for 6-K for foreign issuers) to report material cybersecurity incidents. The Commission adopted many of the reporting requirements proposed in the March 2022 draft of the Regulations and discussed in our prior blog post. Notably, the obligation to disclose information regarding the Board of Directors' cybersecurity expertise was eliminated from the final Regulations based on feedback from commentors who objected to this requirement. In the coming days, we will publish a thorough article regarding public companies' new reporting obligations, but in this post we briefly summarize the new requirements adopted.

Cybersecurity Risk Management

The adopted Regulations will require public companies to provide disclosure regarding their "processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes." The final Regulations eliminate the requirement to disclose policies and procedures for the identification and management of risks from cybersecurity threats, responding to commentors who argued that disclosure of such information would provide details which could be exploited by threat actors. Additionally, the requirement to disclose "processes," reflects the Commission's acknowledgement that such controls are not always codified in formal policies and procedures. Under the adopted Regulations, public companies will still be obligated to make clear whether a risk assessment program is in place with "with sufficient detail for investors to understand the registrant's cybersecurity risk profile." The Commission also notes that the requirement to disclose "processes" eliminates the question of whether companies without formal policies and procedures will have to disclose this fact.

Notwithstanding the fact that the requirement to disclose policies and procedures has been eliminated, the obligation to adopt policies and procedures, as well as technical security controls would still apply to covered entities in various regulated industries. For example, the New York

Department of Financial Services Cybersecurity Regulations and Gramm-Leach Bliley Act Safeguards Rule require such controls for financial institutions. Covered Entities and Business Associates regulated under the Health Insurance Portability and Protection Act are obligated to adopt such controls under the HIPAA Security Rule. Accordingly, while the Commission does not explicitly require companies to adopt specific security controls (such as policies, procedures and technical safeguards), doing so is required by various regulations and a best practice for all organizations.

Cybersecurity Governance

Under the final Regulations, public companies' Form 10-Ks must: (1) "[d]escribe the board of directors' oversight of risks from cybersecurity threats" as well as "any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats," including "the processes by which the board or such committee is informed about such risks"; and (2) "[d]escribe management's role in assessing and managing…material risks from cybersecurity threats[.]" The Commission provided a non-exclusive list of items that should be addressed in the disclosure of management's cybersecurity risk management responsibilities. These include:

- whether certain positions or committees are responsible for assessing and managing cybersecurity risks, including the expertise of the personnel or committees satisfying this role;
- how the relevant personnel or committees are informed about and monitor potential cybersecurity incidents; and
- whether such risks are reported to the board of directors.

Material Cybersecurity Incidents

Among the proposed disclosure requirements that caused considerable consternation was the proposed obligation to publicly disclose material cybersecurity incidents on Form 8-K within 4 business days. The deadline to report incidents will be calculated from the date that the company determines that the incident is material. Like other issues in the securities regulation context, materiality will mean that "there is a substantial likelihood that a reasonable shareholder would consider [the incident] important in making an investment decision." The Commission notes that a "series of unauthorized occurrences", while not material by themselves, may amount to a reportable material cybersecurity incident. Accordingly, material cybersecurity incidents should be "construed broadly."

Board of Directors' Cybersecurity Expertise

The proposed Regulations would have required disclosure of the cybersecurity expertise of public companies' boards of directors on registrants' Form 10-K, as well as in proxy or other information statements regarding the election of directors. Heeding objections of commentors, this requirement was not adopted in the final Regulations. As the Commission noted, "effective cybersecurity processes are designed and administered largely at the management level, and … directors with broad-based skills in risk management and strategy often effectively oversee management's efforts without specific subject matter expertise, as they do with other sophisticated technical matters."

Conclusion

While some of the most discussed disclosure requirements (like board of directors' cybersecurity expertise) were not adopted, the new Regulations will still have substantial impact on organizations. Obligatory reporting regarding cybersecurity processes, risk management and governance will place pressure on organizations to ensure that their cybersecurity programs are appropriately tailored to ensure positive features can be reported in periodic disclosures. Failure to do so could likely lead to additional regulatory scrutiny in the event of a security incident or allegations of failure to discharge fiduciary duties by boards of directors in shareholder derivative lawsuits. Additionally, reporting material cybersecurity incidents in real-time will up the ante with respect to appropriate incident management. Careful disclosure will be required to ensure that such disclosures do not invite increased liability.

To ensure that your organization can make favorable disclosures, conducting periodic risk assessments (like those required by the NYDFS Cybersecurity Regulation, GLBA Safeguards Rule and HIPAA Security Rule) to identify security program gaps and prioritizing remediation of such deficiencies based on the companies' threat profile and the risks such deficiencies pose will be critical to protecting the organization from additional scrutiny and liability. If your organization is not in a regulated industry subject to specific cybersecurity regulations, your program should be benchmarked against a common cybersecurity framework (like NIST CSF or the CIS CSC) to ensure that all appropriate security controls are applied, as appropriate to your organization. Consider conducting such an assessment at the direction of outside counsel to enable counsel to provide legal advice with respect to the sufficiency of your security controls under applicable law or regulation. Having counsel direct the investigation will also protect negative findings with attorney-client privilege, to the extent possible. Attention should also be paid to your cybersecurity governance structure to ensure that appropriate oversight can be conducted by the board of directors. Finally, vulnerability management and event detection should be prioritized, in light of the short data breach reporting deadlines required under the Regulations. Stay tuned for additional analysis on this topic in the coming days and an invitation to a webinar on the implications of the Regulations in September.

National Law Review, Volume XIII, Number 209