Blogs
February 16, 2023
Public Chatter

The Coming Cybersecurity/Climate Disclosure Rules: Time to Reevaluate Your Disclosure Controls?

With the SEC's final cybersecurity and climate disclosure rules just around the bend, and with increased scrutiny of disclosure already required under current rules, it's fair to ask yourself whether it's time to reevaluate your disclosure controls and procedures (DCPs). While the exact requirements of the final rules remain unknown, the picture has been painted with a broad enough brush that you can start thinking about reevaluating DCPs to ensure you aren't caught unawares when the final rules are released.

The Exchange Act of 1934 requires public companies to maintain and periodically evaluate the effectiveness of their DCPs as they relate to financial and nonfinancial disclosures in SEC filings. For various reasons, companies commonly extend DCP to cover significant voluntary disclosures as well.

Given the expanded scope of required disclosures expected under the new rules, companies should reevaluate their DCPs to ensure cybersecurity and ESG matters are adequately captured. Here are five things that companies should keep in mind:

1. **Determine what data to collect.** Companies must determine what data to capture, and until the exact parameters of the final rules are known, should focus on the data most material to their business and industry. Companies can consider industrywide standards or metrics and whether key investors have preferred reporting frameworks. For example, BlackRock asks companies to report using the framework developed by the TCFD, supported by industry-specific metrics, such as those identified by SASB.
2. **Establish data-gathering procedures and systems.** Companies need to establish procedures for how data will be collected, where it is sourced, and how it is stored. Company personnel will need to be assigned responsibility over newly implemented procedures and data collection. Depending on the size and complexity of the data to be gathered, automated data management systems offer advantages over manual collection and storage methods. If companies intend to seek third-party assurance over their data, the procedures and systems need to be of sufficient quality and formality to enable testing by third parties.
3. **Determine how data and resulting disclosures will be reviewed and verified.** Companies must put in place procedures to vet the completeness and accuracy of the data collected and resulting disclosures. For example, internal controls and segregation of duties should be implemented to prevent and detect data fraud; also, certification and/or sub-certification procedures can be established whereby company personnel review and certify disclosures pertaining to their respective areas of responsibility. At the end of the day, the data and disclosures should be comparable across time, across communication channels (e.g., Form 10-K vs CSR Report), and amongst peers.
4. **Talk with your outside auditors and/or consultants.** Audit firms and consultants can help design internal controls and procedures or provide assurance services over data and disclosures. There are a growing number of technology providers to help companies collect climate-related data, as noted recently in this **Reuters article.**
5. **Determine the role of the disclosure committee.** As cybersecurity and climate disclosures are incorporated into DCPs, companies should consider the role their existing disclosure committee will play in the DCP structure. Approaches vary from company to company; some opt to establish separate, stand-alone, subject-specific disclosure committees, while others simply expand the scope of their existing

disclosure committee or create a subcommittee to capture the new disclosure topics.

If the existing disclosure committee is tasked with overseeing new cybersecurity and climate disclosure topics, the disclosure committee will need to be informed on such topics.

While a major overhaul of disclosure committee membership may be premature—as **Broc recently blogged**—disclosure lawyers and existing members of the disclosure committee will need to study up on cybersecurity and climate change. Cybersecurity and ESG experts within the company can still be tasked to review disclosures and otherwise provide help.

Explore more in

Corporate Law
Blog series

Public Chatter

Public Chatter provides practical guidance—and the latest developments—to those grappling with public company securities law and corporate governance issues, through content developed from an in-house perspective.

View the blog