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

SEC Finalizes New Data Breach Reporting Rule; NIST Releases Cybersecurity Framework 2.0

Article By:

Sheila A. Millar

Tracy P. Marshall

How should companies respond to and report data security breaches nationally? What cybersecurity practices and procedures reflect current best practices? Two federal agency actions provide new rules and guidance and show that the cybersecurity landscape is changing. First, the U.S. Securities and Exchange Commission (SEC) adopted new rules earlier this month that will (among other things) require publicly-traded companies to disclose "material" cybersecurity incidents on SEC Form 8-K within four business days and make certain cybersecurity disclosures. Second, the National Institute of Standards and Technology (NIST) recently released its latest Cybersecurity Framework, which now includes a section on corporate governance. Cybersecurity issues are directly related to environmental and social governance (ESG) reporting issues and are increasingly important to businesses from a compliance and governance standpoint. The new SEC requirements have garnered industry criticism, and industry organizations are seeking a delay in the September 5, 2023, effective date.

SEC Finalizes Data Breach and Cybersecurity Reporting Rules

On August 4, 2023, the SEC published final rules in the Federal Register on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure governing cybersecurity disclosures by publicly traded companies as well as corporate processes for managing and responding to cybersecurity risks. The SEC's stated goal is "to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934." The final rules add disclosure obligations that go beyond the SEC's 2018 Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Interpretive Release), which outlines steps that public companies should take when preparing disclosures about cybersecurity risks and incidents. A companion fact sheet was also published on the SEC website. The final rules are slated to take effect September 5, 2023.

The final rules outline specific disclosure obligations in annual or other reports, such as:

- The material aspects of the nature, scope, and timing of the incident, the material impact or

reasonably likely material impact of the incident on the company, including its financial condition and results of operation;
- The company's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant; and
- The board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

The trigger that starts the 4-business day "clock" for a cybersecurity incident disclosure is when a company determines that the incident is "material"; and a materiality determination should be made "without unreasonable delay" after discovery of the cybersecurity incident. The SEC did not define or provide examples of what constitutes a "material" cybersecurity incident but stated that "materiality" will be consistent with applicable case law. (The standard for materiality was established by the U.S. Supreme Court in TSC Industries, Inc. v. Northway Inc., 426 U.S. 438 (1976): "there must be a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available.") A disclosure may be delayed only if the U.S. Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety, and registrants must follow specific procedures to request such a delay.

Issuance of the final rules follows a public comment period that began with the SEC's Notice of Proposed Rulemaking on March 9, 2022. The SEC received more than 150 comments, many of which expressed concern that public disclosure was inconsistent with industry security best practices and that premature disclosure of a breach could make companies more vulnerable to attacks by bad actors. Registrants other than smaller registrants must begin reporting material cybersecurity incidents beginning December 18, 2023; smaller registrants have an additional 180 days to comply. "Smaller reporting companies" were defined previously by the SEC to include a company that 1) has a public float of less than $250 million, or 2) has less than $100 million in annual revenues and no public float or a public float of less than $700 million.

The SEC vote to finalize the rules was 3-2. Dissenting, Commissioner Hester Peirce commented, "The fast timeline for disclosing cyber incidents could lead to disclosures that are tentative and unclear, resulting in false positives and mispricing in the market" and could tip off cyber criminals. She objected in particular to the narrow exemption to disclosures for law enforcement reasons and the cumbersome procedures for requesting a delay in reporting. Also dissenting was Commissioner Mark Uyeda, who stated, "rather than using a scalpel to fine-tune the principles-based approach of the [SEC's] 2018 Interpretive Release … the amendments swing a hammer at the current regime and create new disclosure obligations for cybersecurity matters that do not exist for any other topic."

While the SEC's goal of increased transparency is an important one, prematurely rushing to disclose sensitive information may not be in anyone's best interests and could provide a roadmap of internal vulnerabilities to hackers before a company has adequate opportunity to investigate the situation and determine next steps. The U.S. Chamber of Commerce recently wrote to the Chair of the SEC seeking a 12-month delay in the effective date and recommending a number of additional action steps to obtain additional input from industry and to minimize information flows that might benefit hackers.

NIST Releases Cybersecurity Framework 2.0

Another cybersecurity development important for companies in managing and governing cybersecurity risks is NIST's release of a draft Cybersecurity Framework 2.0 (CSF 2.0) on August 8, 2023. CSF 2.0 is an updated version of NIST's 2014 Cybersecurity Framework (Framework), a widely used tool that helps organizations navigate and manage cybersecurity risk. CSF 2.0 shifts the Framework's focus from critical infrastructure entities to all organizations, regardless of type or size.

Key updates include adding a new governance function to the Framework's original five functions (identify, protect, detect, respond, and recover) and expanded guidance for implementing CSF 2.0. The governance function emphasizes that "cybersecurity is a major source of enterprise risk, ranking alongside legal, financial and other risks as considerations for senior leadership" and helps organizations make important internal decisions and implement processes to support their cybersecurity strategy. Expanded guidance for implementing CSF 2.0 is intended to help organizations create profiles tailored to particular situations.

NIST seeks comments on whether the draft CSF 2.0 is in line with current and anticipated future cybersecurity challenges and aligns with leading practices and guidance resources. The deadline for comments is November 4, 2023. NIST anticipates publishing the final CSF 2.0 in early 2024.

National Law Review, Volumess XIII, Number 237