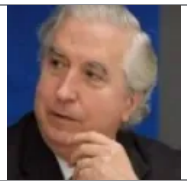

John C. Coffee, Jr. – Mass Torts and Corporate Strategies: What Will the Courts Allow?

By John C. Coffee, Jr.

Compliance's Next Challenge: Polarization

By Miriam H. Baer

Will the Common Goo Guys Come to the Shootou in SEC v. Jarkesy? And Why It Matters

By Eric W. Orts

Editor-At-Large
Reynolds Holding

THE CLS BLUE SKY BLOG

COLUMBIA LAW SCHOOL'S BLOG ON CORPORATIONS AND THE CAPITAL MARKETS

Editorial Board
John C. Coffee, Jr.
Edward F. Greene
Kathryn Judge

Skadden Discusses a Board's Role in Oversight of Cybersecurity Risks

By Anita B. Bandy, Brian V. Breheny, Raquel Fox, William Ridgway and David A. Simon February 28, 2024

Comment

Key Points

- New SEC rules from 2023 require public companies to report material cybersecurity incidents promptly and detail their cybersecurity risk management strategies in annual reports — requirements that increase the risk of litigation over misstatements relating to cybersecurity.
- The fallout from the SEC's enforcement action against SolarWinds and shareholder litigation over the company's alleged failure to manage cybersecurity risks highlight the need for thoughtful board governance in this area.
- Boards should review how oversight responsibility for cybersecurity risk is assigned and coordinated within the board and with management to facilitate clear lines of communication in the event of a cybersecurity incident.

What role are boards expected to play in protecting their companies against cyberattacks?

New rules issued by the Securities and Exchange Commission (SEC) and an enforcement action by the agency against SolarWinds, a software developer that was the victim of a serious cyberattack, provide detailed guidelines. They make clear that directors need to understand the risks and actively engage in cybersecurity oversight. The SEC's actions are also likely to shape the expectations of shareholders, customers and other stakeholders.

New SEC Cyber Disclosure Rules in a Nutshell

Overview

The SEC adopted final rules in 2023, which are intended to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and incident reporting by public companies. Specifically, the amended rules require:

- Prompt public reporting of material cybersecurity incidents on Form 8-K.
- Disclosures in annual reports about the company's processes for identifying, assessing and managing the risks of cybersecurity threats, management's role in assessing and managing those risks, and the board's oversight of cybersecurity risks.

For companies with public floats of more than $250 million, the Form 8-K incident disclosure obligations took effect on December 18, 2023. For those companies, the cybersecurity risk management, strategy and governance disclosures must be included in annual reports for fiscal years ending on or after December 15, 2023 — and thus, for many companies, in annual reports issued in early 2024.

Key Considerations for Boards of Directors

Incident reporting. Under the new rules, a company must disclose a "cybersecurity incident" experienced by the company within four business days of determining that the incident is material.

This requirement has led many companies to evaluate whether their current incident response and disclosure procedures are designed to help ensure compliance with the rules. Management teams and boards are asking whether their company's procedures are integrated and designed to facilitate

streamlined communication between cybersecurity business functions, management and the board in the event of a cybersecurity incident and any steps the board or a committee would need to take in its oversight role.

Cybersecurity governance. Annual reports must now disclose information on the board's oversight of cybersecurity risk management. In particular, companies must describe:

- The board's oversight of risks from cybersecurity threats and, if applicable, any board committee or subcommittee responsible for that oversight.
- How the board or board committee is informed about such risks.

Accordingly, boards should review how oversight responsibility is assigned within the board and make sure that board and committee discussions regarding cybersecurity risks are documented. Those discussions should include regular briefings and updates from management.

The detailed disclosure requirements under the new rules will necessitate robust oversight by boards.

SEC Cyber Litigation and Enforcement: SolarWinds

Companies with inadequate board oversight of cybersecurity practices may face serious consequences.

On October 30, 2023, the SEC filed a complaint against SolarWinds, a software development company, and Timothy Brown, its chief information security officer (CISO), alleging that both SolarWinds and Brown made materially misleading statements and omissions about the company's cybersecurity practices and risks. The SEC claimed this ultimately led to a drop in SolarWinds' stock when a large-scale cybersecurity attack known as SUNBURST was revealed.

The SEC's complaint alleges that SolarWinds and Brown inaccurately claimed on a website security statement that the company followed cybersecurity standards like the National Institute of Standards and Technology (NIST) Cybersecurity Framework, used Secure Development Lifecycle practices (industry-developed standards to minimize software vulnerabilities), enforced strong password policies, and maintained adequate access controls. The SEC also alleged that SolarWinds's SEC filings, including the first disclosure of the SUNBURST incident, included only generic and hypothetical statements that failed to address known cybersecurity risks and vulnerabilities.

The SEC also accused SolarWinds of having deficient cybersecurity controls and known vulnerabilities that left its systems susceptible to attack. Before the attack, SolarWinds and Brown purportedly knew about vulnerabilities and attacks involving its Orion software, used by thousands of SolarWinds customers, but these were not remediated or disclosed.

The SolarWinds case is the first time the SEC has charged a CISO with fraud and highlights the increasing importance of cybersecurity under federal securities law. The SEC's complaint seeks not only corrective actions but also significant penalties, including injunctions and a prohibition against Brown serving as an officer or director of any public company. These charges reflect how seriously the agency views these alleged infractions.

In addition to the SEC's action, two shareholder derivative actions were filed against SolarWinds's directors for failure to oversee operations, and the company agreed to a $26 million settlement in a securities class action filed by its shareholders. The derivative suits were dismissed.

Board and Senior Executive Cyber Risk and Disclosures Checklist

The rules and the SolarWinds case suggest certain basic steps boards should take.

- **Evaluate internal controls:** The SolarWinds action underscores the need for companies to scrutinize internal controls relating to cybersecurity. Regulators, customers and the market expect certain market-standard security practices, like NIST. Companies should develop mechanisms for assessing and elevating issues and ensure that internal cybersecurity weaknesses are promptly addressed, given adequate resources and are promptly brought to the attention of counsel responsible for disclosures. Third-party testing and assessments are critical to identifying gaps in those controls and processes.
- **Proper cybersecurity oversight is in place:** Responsibility for the company's cybersecurity risk should be clearly assigned and coordinated within the board and have established procedures. The board or committee overseeing cyber issues should ensure that management has conducted tabletop exercises to test and assess the company's incident response and its processes for disclosures.
- **Consider the SEC's expansive view of materiality:** Whether a cybersecurity event is considered material will hinge on quantitative and qualitative factors, including:
  - The extent to which the attack uncovered significant deficiencies in the company's overall cybersecurity infrastructure.
  - The extent to which the attack shows weaknesses in systems associated with Sarbanes-Oxley (SOX) compliance and financial reporting, including the integrity of the information processed by these systems.
  - The scope of sensitive customer or employee data compromised.
  - Costs relating to remediation.
  - Loss of a material contract or customer business.

- Reputational harm.
- The impact on the company's stock when an announcement was made.

- **Evaluate the risks of statements and disclosures beyond SEC filings:** In the Solar Winds litigation, the SEC leaned heavily on the company's Security Statement, which was included on its website, alleging that it contained misstatements about the company's compliance with cybersecurity standards, its software products, and password policy and access controls. The lesson here: Companies must evaluate all their public statements, not just those in SEC filings.
- **Validate all cybersecurity assurances:** Publicly disclosed cybersecurity assurances must be defensible and consistent with the reality of the company's cyber health.
- **Weigh the cumulative cyber risks:** Individual cybersecurity issues that are not material on their own are evaluated alongside prior incidents to provide context for current incidents, ensuring that the full picture of cyber risks is conveyed to investors.
- **Involve the CISO in the disclosure process:** The company's CISO should be involved in the disclosure process to assess and explain the technical nature of any cybersecurity risks.
- **Distinguish actual from hypothetical risks:** Disclosures should accurately distinguish between actual cyber events and potential, hypothetical risks. Known exploits or vulnerabilities should not be downplayed as merely possible or speculative when there is evidence to suggest otherwise.

What Factors May Make a Cyberattack "Material"?

- Significant losses or reduced revenue.
- Change in stock price.
- Focus by management, analysts and/or investors on cyber-related issues during earnings calls.
- Significant impact to company's operations, including costs of remediation associated with a breach or cyber intrusion.
- Unauthorized access to significant amount of sensitive data, such as personally identifiable information of customers.
- Impact to the company's Sarbanes-Oxley financial reporting systems.
- Harm to company's reputation.
- Data integrity issues.
- Pending or anticipated litigation stemming from the incident.

This post comes to us from Skadden, Arps, Slate, Meagher & Flom LLP. It is based on the firm's article, "Emerging Expectations: The Board's Role in Oversight of Cybersecurity Risk," dated Winter 2024, and available here.