CARTER/LEDYARD

our resources

Cybersecurity Risk Management Enforcement – Pendulum Swings

March 07, 2025

The Securities and Exchange Commission (the "SEC") recently announced the creation of a Cyber and Emerging Technologies Unit ("CETU") that will focus on fraudulent conduct in cybersecurity, digital assets, and emerging technologies such as artificial intelligence. For reporting issuers, the announcement indicates that the new unit will focus on combatting fraud and other "cyber-related misconduct," including "public issuer fraudulent disclosure relating to cybersecurity."

The unit's announced focus on "fraudulent" cybersecurity disclosures marks a potential shift from the SEC's recent enforcement approach, which we will discuss below.

SEC's Cybersecurity Enforcement since 2023

On July 25, 2023, the SEC adopted new rules for reporting companies regarding cybersecurity risk management. The SEC enforced accurate disclosure of risks. In October 2024, the SEC charged four current and former public companies – Unisys Corp., Avaya Holdings Corp., Check Point Software Technologies Ltd, and Mimecast Limited – with making materially misleading disclosures regarding cybersecurity risks and intrusions. The SEC also charged Unisys with disclosure controls and procedures violations.

In October 2024, the four companies agreed to pay the following civil penalties to settle the SEC's charges:

- Unisys paid a $4 million penalty;
- Avaya. paid a $1 million penalty;
- Check Point paid a $995,000 penalty; and
- Mimecast paid a $990,000 penalty.

These settlements were consistent with SEC policy which evolved prior to the 2023 rules. For example, in August 2021, the SEC announced a settlement with Pearson plc, for making a misleading risk factor disclosure about data breaches. Pearson's SEC filing included a statement that a data privacy incident was a risk that "could result" in a major breach. The SEC alleged that the SEC filing and a subsequent media statement were misleading because Pierson characterized a known harm as a hypothetical risk.

The SEC's order against Unisys found that the company described its risks from cybersecurity events as hypothetical despite knowing that it had experienced two SolarWinds-related intrusions involving exfiltration of gigabytes of data. The order also found that these materially misleading disclosures resulted in part from Unisys' deficient disclosure controls. The SEC's order against Check Point found that it knew of the intrusion but described cyber intrusions and risks from them in generic terms.

In these settlements, the SEC mostly relied on negligence-based fraud claims under the Securities Act or internal controls charges under the Exchange Act stemming from a company's inadequate policies and procedures regarding the escalation of information regarding a cybersecurity incident. Importantly, it did not require *scienter*, the intent to make false statements.

The SEC's announced priorities in connection with CETU signal a narrowed focus on investigating and bringing cybersecurity disclosure actions against reporting companies to those cases where the conduct rises to a higher level of misconduct – i.e., *intentionally* fraudulent representations.

A Potential Step-down of the Cybersecurity Rules

The Cybersecurity Rules impose broad disclosure requirements on reporting companies aimed at enhancing and standardizing disclosures regarding cybersecurity incidents and controls.

Both Acting Chair Mark T. Uyeda and Commissioner Hester Peirce dissented at the time from the adoption of the Cybersecurity Rules, criticizing the requirements as unnecessary, immaterial and burdensome.

On October 22, 2024, Uyeda and Peirce issued a joint dissent heavily criticizing charges brought against companies for allegedly making materially misleading disclosures regarding cybersecurity.

The dissent characterized the enforcement allegations as being of two types:

(1) Failing to disclose material information (in the cases of Avaya and Mimecast); and
(2) Failing to update an existing risk factor in response to a cyberattack (in the cases of Check Point and Unisys).

The dissent disagreed that there were material omissions and believed it highly unlikely that investors would view them as material especially since some of the incidents were already reported in the media. Therefore, they considered the focus to be wrongly directed on the immaterial details regarding the incidents themselves rather than their overall impact.

Acting Chair Mark T. Uyeda and Commissioner Hester Peirce also discounted certain claims by the SEC of companies allegedly framing cybersecurity events as hypothetical. They countered that there should have been a clearer explanation on why any of the alleged omissions were material from a securities law perspective.

The dissent concluded that the majority failed to apply a "reasonable investor" standard in each of these orders.

There is uncertainty as to whether the SEC, when the new Chairman and new Commissioners are in place, will repeal or otherwise revise the Cybersecurity Rules. Some clues could be derived from the way they looked at other somewhat similar rules. On February 11, 2025, Acting Chair Uyeda announced that the SEC will not defend its climate disclosure rules that are currently being challenged in the Eighth Circuit. It is unclear whether the other Commissioners will take a similar stance and ultimately consider repealing, or otherwise limit the enforcement of the Cybersecurity Rules. There are of course fundamental differences between the climate change rules and the Cybersecurity Rules, and the challenge to the climate rules goes much deeper. Critics argue the SEC does not have the authority to require climate-related disclosures without specific congressional approval, and some argue that the rules violate companies' First Amendment rights, issues that are not as relevant to cybersecurity disclosure or enforcement.

Coping with Future Potential SEC Cybersecurity Enforcement

- The SEC remains committed to cybersecurity enforcement, but the specifics are still developing. The creation of the CETU confirms that cybersecurity disclosures remain a key area of scrutiny.

- There is a potential shift towards focusing on "fraudulent" cybersecurity disclosures, possibly moving away from past actions that heavily emphasized negligence-based charges.
- This could mean a narrower scope for SEC investigations, charges, and penalties related to cybersecurity disclosures.
- Companies must maintain robust disclosure and escalation procedures for cybersecurity incidents.
- The SEC expects companies to have well-defined disclosure practices and committees to ensure timely and accurate information flow for materiality assessments.

In simpler terms:

The SEC is still very interested on cybersecurity, but the SEC may change how it enforces the rules. It might **focus more on companies that intentionally lie about cybersecurity issues or fail to promptly disclose such issues.**

When adopting its Cybersecurity Rules, the SEC recognized that disclosure of immaterial cybersecurity issues may "divert investor attention" and result in "mispricing of securities," and there is concern that the practical effect of enforcement actions will be an increase in filings reporting on immaterial events.

Regardless, companies still need to have policies and procedures in place to address and report material cybersecurity incidents.

* * *

related professionals

Guy Ben-Ami / Partner
D 212-238-8658
benami@clm.com