Davis Polk

SEC charges public companies with inadequate disclosures in aftermath of the SolarWinds cyberattack

October 30, 2024 | Client Update | 9-minute read

The SEC announced settled enforcement actions against several victims of the SolarWinds hack, alleging that they downplayed the extent to which they were impacted by the intrusions. The actions highlight the current SEC's aggressive posture in evaluating cyber disclosures.

Background

On October 22, 2024, the SEC instituted settled actions against four current and former public companies impacted by the 2020 SolarWinds software hack – Unisys Corp. (Unisys), Avaya Holdings Corp. (Avaya), Check Point Software Technologies Ltd (Check Point), and Mimecast Limited (Mimecast). The SEC alleged that the companies made materially misleading disclosures regarding cybersecurity risks and intrusions relating to the SolarWinds hack, and that one of the companies (Unisys) also had deficient disclosure controls and procedures.

The SolarWinds hack, attributed to Russia's intelligence agencies, involved the insertion of malicious code known as SUNBURST into SolarWinds' Orion software, which was then distributed to thousands of customers, including private companies, nonprofits and various government agencies. The threat actors used sophisticated tactics to hide in the SolarWinds network for over a year, including a legitimate code-signing certificate, various command and control servers, and custom malware designed for obscurity.

For several years, the SEC has conducted a wide-ranging investigation regarding the SolarWinds hack, including a voluntary request asking hundreds of public companies to inform the SEC how they were impacted by the hack. In October 2023, the SEC brought a much-publicized enforcement action against SolarWinds and the vice president of its information security group, alleging that the company, the primary victim of the cyberattack, made misleading disclosures regarding the security of its software and cybersecurity practices and that the company also had deficient internal accounting and disclosure controls. We previously discussed a decision by the federal judge overseeing the SEC's litigation, in June 2024, dismissing key aspects of the SEC's disclosure and internal controls allegations. With these latest enforcement actions, the SEC has broadened its focus to the downstream victims of the breach.

In a troublesome development, the SEC's theory in some of these cases suggests that it will expect disclosure that goes beyond what is required by the SEC's cybersecurity disclosure rules for public companies, adopted in July 2023, which we covered here and predate the recent settled actions. As summarized below, the SEC alleged that some of the companies failed to disclose details regarding cybersecurity intrusions—such as the identity of a threat actor or the number of customers impacted—that are not specifically required to be disclosed under the current rules. While the materiality of any particular fact must be considered on a case-by-case basis, our concern is that companies may feel pressured by these enforcement cases to disclose details they believe are immaterial, and thus not required to be disclosed under the SEC's disclosure rules. This could undermine the effectiveness of the new rules by flooding investors with immaterial details, making it more challenging for them to identify the material events and risks that might impact their investment decisions.

SEC settlements

The SEC's actions focus on the disclosures made by the four settling companies after they came to learn of the SUNBURST cyberattack. The SEC alleged that the companies failed to provide accurate disclosures regarding the impact of the attack

and minimized the scope and severity of the intrusions. The SEC alleged negligence-based fraud violations against each of the companies—the SEC did not allege intentional fraud and it did not bring claims against any individuals. The SEC acknowledged that the settling companies cooperated with the SEC's investigations and imposed civil penalties ranging from $990,000 to $4 million.

— **Unisys Corp.** Unisys is a global provider of information technology services and solutions. The SEC alleged that the company made materially misleading disclosures when it described its cybersecurity risks as "hypothetical" in its annual reports despite knowing that the SolarWinds hack had resulted in the loss of a substantial amount of sensitive data. This type of claim is not a new one. However, in addition to this, the SEC further alleged that the company lacked adequate disclosure controls and procedures because the company's incident response allegedly did not reasonably require cybersecurity personnel to escalate information around cybersecurity incidents to disclosure decision-makers. Unisys cooperated and provided comprehensive presentations to the SEC, summarizing key factual issues and implemented remedial measures. The SEC imposed a $4 million penalty.

— **Avaya Holdings Corp.** Avaya, through its subsidiaries, provides digital communications software solutions and services for global businesses. The SEC found that Avaya's post-breach disclosures downplayed the severity of the SolarWinds attack, omitting key details about compromised proprietary information. In particular, the company had disclosed that a threat actor had accessed a "limited number of [the] company's email messages" when the threat actor had also accessed at least 145 files in its cloud file sharing environment. The SEC also alleged that the company failed to disclose all material facts known to the company from its internal investigation, including that the threat actor was likely a nation-state actor. The SEC's settled order credited Avaya's cooperation, which included conducting an internal investigation and sharing its findings with the SEC staff, as well as its enhancements to its cybersecurity controls. The SEC imposed a $1 million penalty. Notably, the SEC's new cybersecurity disclosure rules do not require identification of the threat actor, while the enforcement action suggests that the SEC does view the identity of the threat actor as a required disclosure.

— **Check Point Software Technologies Ltd.** Check Point is a technology company providing cybersecurity solutions for IT companies worldwide. The SEC alleged that Check Point became aware of the SolarWinds Orion hack after conducting an internal investigation, determining that it had been the target of malicious activity by a threat actor. While the company had a robust risk factor disclosure about cyber threats that stated that the company had been subject to prior hacks, the SEC alleged that the company's disclosures regarding cybersecurity were "virtually unchanged" from its prior disclosures, and the company continued to describe the existence of intrusions in only generic terms and failed to disclose new cybersecurity risks relating to the SolarWinds Orion hack. Again, the SEC cybersecurity disclosure rules for public companies do not require updating of risk factors that are otherwise accurate, yet the SEC enforcement action suggests that some updating is required. The SEC imposed a penalty of $995,000.

— **Mimecast Limited.** Mimecast is a cloud security and risk management services company. According to the SEC's order, the company came to learn that it had been compromised by the same threat actor behind the SolarWinds Orion hack. Among other things, the threat actor had exfiltrated a Mimecast-issued authentication certificate used by a portion of its customer base, compromised five customers' cloud platforms, and accessed internal email and source code at the company. Mimecast disclosed this cybersecurity incident in Forms 8-K and certain details of the incident but, according to the SEC, did not disclose "the number of customers whose credentials or server and configuration information were accessed by the threat actor" and did not describe "the nature of the code, nor quantify the amount of source code exfiltrated." As a result, the SEC alleged that the company, despite publicly acknowledging the cybersecurity incident, had minimized the attack. Again, the SEC's cybersecurity rules do not require disclosure of details such as the number of customers affected, yet the SEC enforcement action suggests that type of disclosure is required. The SEC levied a penalty of $990,000.

Dissent

SEC commissioners Hester Peirce and Mark Uyeda dissented from the settled proceedings on the grounds that the companies, in their view, had provided sufficient material information to investors. They criticized the SEC's approach as "playing Monday morning quarterback" and unfairly engaging in a "hindsight review" of the disclosure decisions. The commissioners cautioned that the SEC's aggressive enforcement approach risked causing companies to disclose immaterial facts to investors out of fear of being second-guessed by the SEC, which would thereby divert investor attention and result in the mispricing of securities – concerns which they said the SEC recognized in the cybersecurity rules adopted in July 2023. The commissioners also suggested that the enforcement actions could undermine the SEC staff's recent guidance steering companies away from disclosing immaterial incidents under Item 1.05 of Form 8-K.

Commissioners Peirce and Uyeda also noted that the allegations against Check Point—that the company had failed to update its cybersecurity risk factor disclosures after becoming aware of a specific cybersecurity event—were similar to the SEC's allegations against SolarWinds, and which had been rejected by a federal judge. That court held that SolarWinds' cybersecurity risk disclosure was sufficient because it had alerted the investing public to the cybersecurity threat faced by the company. The commissioners noted that Check Point's and SolarWinds' risk factor disclosures were "arguably similar."

Key takeaways

These latest resolutions signal that the SEC, under current leadership, will continue to take an aggressive approach toward issuer cybersecurity disclosures despite the mixed result in its pending litigation against SolarWinds. We see a few key takeaways:

— **The SEC will scrutinize materiality judgments with the benefit of hindsight**. Two of the companies in the recent resolutions, Avaya and Mimecast, disclosed in their SEC filings that they had been the target of a specific cybersecurity attack. The SEC's main complaint was that the disclosures did not include additional details about the attack. For instance, among the Avaya allegations was that the company failed to disclose that the threat actor was likely a nation-state actor. The two dissenting commissioners questioned why this detail was material. In the Mimecast resolution, the SEC alleged that the company failed to disclose the number of impacted customers, or the nature or type of source code that had been exfiltrated. Again, the dissenting commissioners questioned why those were material omissions. Judgments about materiality in the aftermath of a cybersecurity breach can be challenging, and in our experience companies engage in good faith deliberations to determine what information should be disclosed to investors. We also have seen that some details quickly become out of date. The SEC's actions highlight that companies crafting cybersecurity disclosures should expect the SEC to second-guess its judgments.

— **The nature of a company's business is relevant to materiality.** Each of the settling companies was in the software or IT business. For those industries, a cybersecurity vulnerability in its software, depending on other facts, might be more likely to be material than other industries because the ability to protect the integrity of its software is, potentially, more central to its business.

— **Cybersecurity risk factor disclosures continue to be an area of focus.** The SEC continues to focus on risk factors using hypothetical wording after a company has seen the risk come to fruition. We previously wrote about a prior enforcement action that involved such a theory, where the SEC alleged that a company disclosed the risk that it "could" have a data privacy breach when it knew it had in fact experienced a breach. The SEC's action against Check Point presents a novel twist in that Check Point made affirmative disclosures that it faced regular cyber intrusion attempts by malicious hackers but that none of those attempts had "resulted in any material adverse impact to [its] business or operations." The SEC viewed this risk factor disclosure as misleading because the company's risk profile "had increased" as a result of the SolarWinds cybersecurity attack. The SEC also criticized the company's risk factor disclosures as "generic" and "not tailored" to the company's particular cybersecurity risks. The case is a reminder that companies should review their risk factors in light of recent experiences and consider whether updates are warranted.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Ning Chiu
+1 212 450 4908
ning.chiu@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

Michael Kaplan
+1 212 450 4111
michael.kaplan@davispolk.com

John B. Meade
+1 212 450 4077
john.meade@davispolk.com

Alain Kuyumjian
+1 212 450 3628
alain.kuyumjian@davispolk.com

Stefani Johnson Myrick
+1 202 962 7165
stefani.myrick@davispolk.com

Fuad Rana
+1 202 962 7053
fuad.rana@davispolk.com
