SEC Enforcement Case Summary
Misleading Disclosures Regarding Cyber Risks & Intrusions

On October 22, 2024, the SEC charged four public companies with making materially misleading disclosures regarding cybersecurity risks and intrusions and charged one company with disclosure controls and procedure violations. Penalties ranged from $990,000 to $4 million. The SEC's Enforcement Head noted that "while public companies may become targets of cyberattacks, it is incumbent upon them to not further victimize their shareholders or other members of the investing public by providing misleading disclosures about the cybersecurity incidents they have encountered."

The SEC noted that Unisys Corp., Avaya Holdings Corp., Check Point Software Technologies Ltd., and Mimecast Limited, each learned that the threat actor likely behind the 2020 SolarWinds Orion hack had accessed their systems without authorization. SolarWinds is a major software company which provides system management tools for network and infrastructure monitoring, and other technical services to hundreds of thousands of organizations around the world. Among the company's products is an IT performance monitoring system called Orion, which had privileged access to IT systems to obtain log and system performance data. In the SolarWinds hack, suspected nation-state hackers gained access to the networks, systems and data of thousands of SolarWinds customers. The breadth of the hack is unprecedented and one of the largest of its kind ever recorded.

Upon learning of the breach, the SEC noted that each of the four firms negligently minimized the cybersecurity incident in public disclosures. In the most egregious case, Unisys received notifications about and discovered compromises in its environment that took place over a 16-month period and involved at least seven network credentials, 34 cloud-based accounts, including those with administrative privileges, and repeated connections into Unisys's network with at least 33 gigabytes of data transferred, and access to cloud-based shared files and mailboxes, including those of senior IT personnel. The SEC order noted that Unisys was aware that its investigations of the compromise involved significant gaps in its ability to identify the full scope of the unauthorized activity due to the lack of availability of forensic evidence. Despite the extent of the breach, Unisys described its risks from cybersecurity events as "hypothetical" in public disclosures.

Avaya stated that the threat actor had accessed a "limited number of [the] Company's email messages," when it knew the threat actor had also accessed at least 145 files in its cloud file sharing environment. The SEC's order against Check Point noted that it knew of the intrusion but described cyber intrusions and risks from them in generic terms. Mimecast minimized the attack by failing to disclose the nature of the code the threat actor exfiltrated and the quantity of encrypted credentials the threat actor accessed.

The SEC Acting Chief of the Crypto Assets and Cyber Unit warned in the press release that "downplaying the extent of a material cybersecurity breach is a bad strategy," and criticized the firms for framing risks as hypothetical or generically when they knew that the risks had already materialized. While these cases involve public company disclosures, investment advisers and private fund managers must also be cautious in downplaying cybersecurity risks or making misleading statements or inferences in risk disclosures where they have experienced material cybersecurity events.

See Summary – https://www.sec.gov/newsroom/press-releases/2024-174