Blogs
August 18, 2021
The SEC Brings Another Cyber Breach Disclosure Case! 5 Things to Consider

For years, we've heard that the SEC's Enforcement Division has been policing cybersecurity breach disclosures and related disclosure controls. The SEC has conducted a number of SEC investigations over that time, but very few of those have seen the light of day. We recently **blogged** a few times about one of those, the SEC's Solar Winds inquiry. A few days ago, the SEC's Enforcement Staff **announced a settlement** resulting in a $1 million civil penalty following a **June action** regarding a disclosure control deficiency relating to a cyber incident. While the factual details of each enforcement proceeding are important for a full understanding of the SEC Staff's position, let's focus on some practical lessons from these actions and some related steps you can take now: 1. **Update hypothetical risk factors**: A good risk factor is broad enough to cover foreseeable hypothetical risks (e.g., a cyber breach "could" result in a material adverse impact) - but also specifically covers adverse events that have actually taken place (e.g., a cyber breach occurred and "had" a material adverse impact relating to XYZ). A disclosure that an event "could" occur when it has actually occurred will receive SEC scrutiny as misleading. And it also essentially fails to provide the liability warning and protection you want from your risk factors.Take a look at your risk factors and focus on reviewing the hypothetical risk disclosures. Have they actually occurred? If so, it is critical to update with the specific situation and details. That could mean something as little as changing a verb or adding specific disclosures and the actual adverse impacts regarding an event that has actually occurred. 2. **Be transparent and accurate**: When announcing a cybersecurity intrusion - or really anything - you must accurately report the event. Understating the scope of the breach or merely hypothetically noting that certain information "may" have been compromised when, in fact, you are aware that your company "was" compromised will be viewed as a misleading statement or an omission of a material fact necessary to make the statement not misleading. 3. **Don't mislead**: It is understandable that, after a breach, companies will want to reassure their customers and the market with statements about their cybersecurity defenses and remediations, but those statements will be subject to scrutiny. Again, you need to be transparent and accurate in your public disclosures and not overstate your defenses or reactions. 4. **Get the info to decision makers**: Make sure that you have effective disclosure controls around cyber events to ensure the relevant information is fully and promptly available to those responsible for SEC disclosures. In my experience, securities lawyers and executives responsible for SEC reporting may not have the technological expertise to fully understand the cyber incident, so it's crucial that outside advisors and internal security personnel fully explain the situation in a way that can be understood by a lay person. Companies often debate on when to disclose based on what is known at the time. Once that judgment is made, it is critical that the disclosure be fully vetted by those versed in SEC disclosures to be sure it's accurate and not misleading. 5. **Foreign private issuers are still subject to SEC disclosure rules**: Although foreign private issuers are exempt from certain SEC rules, it is worth a reminder that their filings with the SEC on 6-K, 20-F, and otherwise must be accurate and not misleading. Foreign private issuers will want to stay current on SEC hot button topics like cybersecurity and ESG disclosures and be sure their disclosure controls and procedures around these topics operate effectively.

Authors

Explore more in

Corporate Law Public Chatter