PUBLICATION

New SEC Rules: Public Companies Must Report Material Cybersecurity Incidents Within Four Business Days

Authors: Alisa L. Chestler
July 27, 2023

It is official. On July 26, 2023, the Securities and Exchange Commission (SEC) passed rules regarding reporting "material cybersecurity incidents" within four business days of the determination, which will surely vex companies for years to come. Public companies and their third-party vendors, including private companies, will feel the effects of these rules in their contracts and negotiations. Let's get into what happened and what companies should do now.

Overview of SEC Rules

Once the regulations are published in the Federal Register, which we expect shortly, public companies will have 30 days to comply. Under the regulations, the SEC will require public companies to report "material cybersecurity incidents" on a Form 8-K within four business days of such a determination. Further, companies will need to provide material information regarding their cybersecurity risk management, strategy, and governance on an annual basis. Below are some initial thoughts to consider in understanding the issues related to the cybersecurity event notification.

- **"Material" Definition.** If you are wondering what qualifies as "material," you are not alone. Management and legal teams need to consider what might be "material" in all sorts of scenarios to help identify the issues in advance. For example, maybe a breach that affects the supply chain is material after one day or maybe it is material after three days. Maybe theft of intellectual property has occurred and while material, does it impact national security and therefore merit a delay?

- **What Needs to be Reported?** Note, this changed from the proposed rules. To the extent known at the time of filing the material aspects of:

  - Nature, scope, and timing; and
  - Impact or reasonably likely impact.

- **Four Business Day Deadline.** Given the short timeframe for reporting and the potential for uncovering new information while investigating an incident, companies should anticipate the potential need to amend and update filings as the facts become clearer. Companies will want to avoid speculation.

- **Also Consider Human Error.** Cybersecurity events are not limited to ransomware and sometimes can just be mistakes in information system configurations. Human error can be a factor, and these should be understood as a part of the planning process.

What Should Companies Do Now?

- All companies should already be conducting incident response exercises. Such exercises should include the important considerations of notifications, including notifications to federal and state regulators and now to the public through the Form 8-K. As time is of the essence, this should be nearly immediate, and a well-practiced response program will be critical. Counsel should have always

been included in the incident response exercise, however now their inclusion in the planning and execution of the exercises is absolutely crucial.

- Companies should also consider the "me too" effect. Imagine your company has recently faced an issue similar to what many faced with the MOVEit breach. That breach may be material for one public company, but not for another public company. This analysis felt more comfortable without a four business day deadline looming. Companies must understand their protocols in these cases.

Our team intends to issue more alerts on this topic as more information becomes available, which will cover a broad array of issues, including corporate governance. You can read the SEC's press release here to learn more about the new rules. If you have any questions about the rules or would like help putting incident response protocols into place for your business, please contact Alisa L. Chestler, CIPP/US, QTE or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.