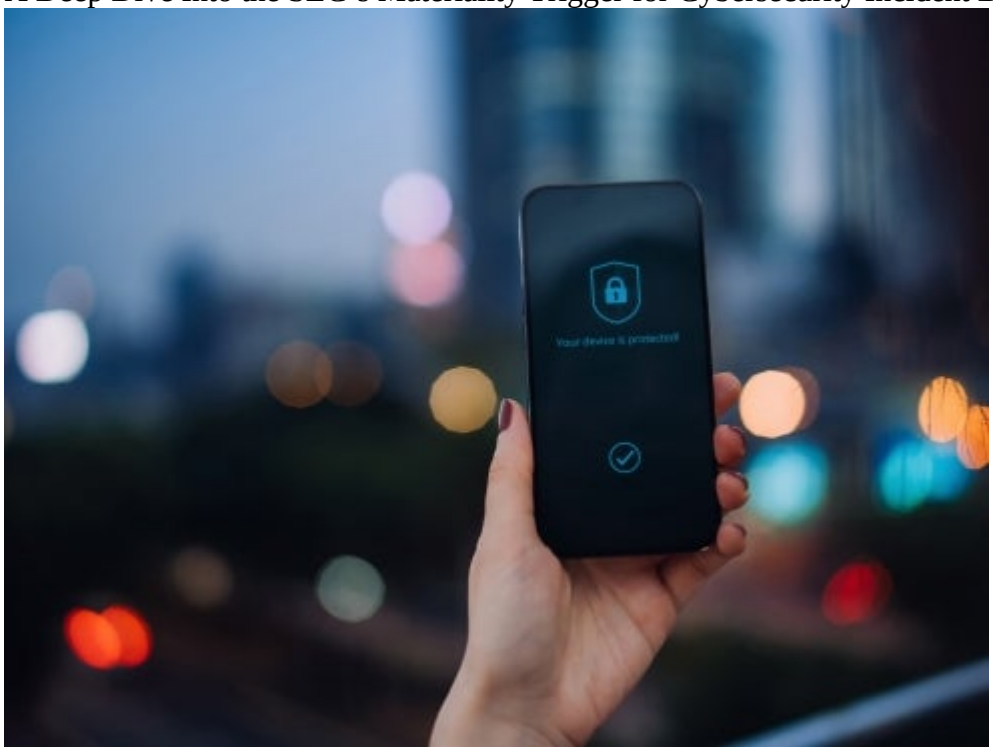
Blogs
September 11, 2023
A Deep Dive Into the SEC’s Materiality Trigger for Cybersecurity Incident Disclosures



The U.S. Securities and Exchange Commission (SEC) adopted final rules relating to cybersecurity disclosure on July 26, 2023, which will take effect on December 18, 2023.

As we outlined in a prior post, the new rule requires public companies to disclose material cybersecurity incidents and to make affirmative representations relating to the organization's cybersecurity risk management, strategy, and governance in annual reports.

As registered entities brace themselves for the SEC's new disclosure requirement, we offer a closer look at the SEC's "materiality" standard as it applies to cybersecurity incidents. Some organizations may need to make significant adjustments into how incidents are handled and assessed in order to meet the fairly strict timelines for disclosure. We expect that properly and accurately assessing the materiality of a given incident will be a complex endeavor, fraught with legal risk.

The Materiality Trigger

As set forth in the SEC's initial proposal and reaffirmed in its publication of the final amendments, cybersecurity incidents trigger the new disclosure requirements when the incident is "material." An incident is "material" when the relevant information—i.e., the description of the incident itself—is information for which there is a **substantial likelihood that a reasonable shareholder would consider it important in making an investment decision,** orwhen it would have **significantly altered the "total mix" of information made available**.These are familiar standards for any public company in the abstract, but will now be applied in a field so new and dynamic that even the SEC has declined to offer a definition of it in the rule. *See* Final Rule ("We also decline to separately define "cybersecurity," as suggested by some commenters. We do not believe such further definition is necessary, given the broad understanding of this term. To that end, we note that the cybersecurity industry itself appears not to have settled on an exact definition, and because the field is quickly evolving and is expected to continue to evolve over time, any definition codified in regulation could soon become stale as technology

develops."). Indeed, the SEC explicitly declined to adopt a cybersecurity-specific definition of "materiality," instead noting that "[c]arving out a cybersecurity-specific materiality definition would mark a significant departure from current practice, and would not be consistent with the intent of the final rules." If the materiality call is close, the SEC advises erring on the side of disclosure, noting that "[d]oubts as to the critical nature of the relevant information should be resolved in favor of those the statute is designed to protect, namely investors." (Footnotes and citations omitted.)

Incident responders tend to think of the "significance" of an incident in terms of one or more of the following: (1) the quantity and quality of data that was accessed (with a focus on the risk of harm to the data subject for an unauthorized disclosure); (2) the level of operational disruption imposed; and/or (3) the existential risk to the company itself. What the SEC's comments make clear, is that these avenues for assessing significance are only some of the ways an incident can be "material." Below, we discuss how the SEC's concept of "materiality" adds new considerations that incident responders, and those engaging with them, may not be in the practice of incorporating. Following that, we discuss some potential pain points in assessing materiality for events that are otherwise "significant" under the more traditional approach to assessing incident severity.

1. Additional Signals That an Incident Is "Material": A Different Type of Harm

The SEC's comments illustrate that the focus of any materiality assessment should be "through the lens of the reasonable investor." In other words, materiality is not limited to a quantifiable amount of access that occurred, or how likely it is that such access would affect consumers, but includes any information connected to an incident that a reasonable investor would want to be aware of, or that would otherwise significantly alter the "total mix" of available information. ***So, while incident responders may typically think of the risk of incident-related harm as the risk that a bad actor might misuse the information to the detriment of data subjects, harm in this context can mean selling a "cybersecurity bill of goods" to the reasonable investor***. This means that certain events, even if the specific occurrence does not seem especially significant or harmful, may still be viewed as harming potential *investors* if the incident is evidence of bad security practices in general. In other words, if an incident reveals a weakness in an organization's security safeguards, but the organization "got lucky" in the incident itself, that "luckiness" does not absolve it of the need to assess whether the weaknesses demonstrated are material when considered more holistically.

A good analogy for this concept is child care. Imagine that you drop your child off every day for day care. There is an incident where your child is struck by another child in the presence of day care staff, who immediately address the issue, called you, and explained the whole situation, why it happened, and what they will do to avoid a future incident. I think we would all expect and demand that. What if, the next day, your child was alone in the same room with that child for 30 minutes, and during that time, the other child threw something heavy at your child, and completely missed. No staff members were present because the childcare center had an insufficient number of professionals on duty, and their practice is to remain open even if understaffed. Material? Wouldn't you as a parent want to be notified of an incident, even though there were no injuries, given that the incident demonstrates a general level of care well below what you expected and paid for? Ultimately, the harm to the parent from the second incident is analogous to the concept of harm inherent to the SEC's "materiality" trigger.

A real world example worth examining is the securities litigation arising out of the widely publicized breach of SolarWinds Corporation's (SolarWinds) ubiquitous network monitoring tool, Orion. This theft of data from SolarWinds and its customers (the Orion Breach) is considered to be a "supply-chain" attack because the malicious hackers targeted SolarWinds primarily to reach their downstream customers.

In the litigation arising out of the Orion Breach, a federal district court considered SolarWinds' motion to dismiss a class action complaint from a class of plaintiffs who purchased SolarWinds securities from October 18, 2018, through December 17, 2020 (a time period leading up to the late 2020 discovery of the breach). *See In re:*

Solarwinds Corp. Sec. Litig., 21-CV-138-RP (W.D. Tex., Mar. 30, 2022). The plaintiffs alleged that the defendants (including SolarWinds, its CEO, CFO, and Vice President of Security Architecture during the class period, as well as two private equity firms each holding approximately 40% of SolarWinds' stock) made material misrepresentations about their cybersecurity during this time period. One of the many representations the plaintiffs complained of were representations by SolarWinds that it maintained a password policy on which employees were trained and with which they complied. This representation was juxtaposed against another incident ***that was not at all related to the actual Orion Breach*** and was not found to be associated with the theft of data, but which nevertheless occurred during the relevant time period.

On November 11, 2019, SolarWinds was notified in writing that a cybersecurity researcher was able to find a password for the update server SolarWinds uses to distribute software updates for its Orion product; that the password was available for approximately one-and-a-half years on GitHub; and that the password itself, "solarwinds123," was incredibly weak. The defendants argued that their prior touting of their cybersecurity posture and practices are not rendered materially misleading simply because they were ultimately breached. The court recognized the accuracy of this argument, but went on to note that the basis for the court's materiality finding is premised differently, as it is based on "separate facts [alleged by the plaintiffs] that the cybersecurity measures at the company were not as they were portrayed, such as the 'solarwinds123' password incident …." Ultimately, the court largely denied the defendants' motion to dismiss, finding that plaintiffs had adequately alleged, *inter alia*, actionable and material misstatements. In other words, in light of affirmative statements the corporation made about its security, the "solarwinds123" incident was found to be plausibly "material," because it arguably showed that "the cybersecurity measures at the company were not as they were portrayed…"

Counsel who are familiar with the Federal Trade Commission's (FTC) approach for assessing data security issues will see parallels. Although the FTC focuses on consumers rather than investors, the issue of whether a security incident calls into question the accuracy of an organization's description of its security practices or its response to an incident, even in the absence of significant harm in fact arising from the incident, is a core component of the analysis under both legal regimes.

What the *SolarWinds* opinion shows is how the concept of materiality to investors can be applied to cybersecurity incidents. And while incidents that would traditionally have been viewed as "significant" for a company would almost certainly be considered "material," information about an incident can also be considered "material" simply because it shows that an organization is not as serious about cybersecurity as it otherwise claims to be. Keep in mind that a primary purpose of the SEC is to prevent unfair asymmetries of information, not to implement good cybersecurity. So, while incident responders traditionally think about sizing an incident based on the "harm" done to an organization, its data, or others, materiality requires companies to assess these same incidents, but with a view to preventing the "harm" to an investor paying for the stock of a company with good security (or security as represented in public statements), while receiving the stock of a company with bad security. Although it remains to be seen exactly how the case law around this issue will play out, the reality is that plaintiffs need only generate a genuine dispute of material fact in order to get to a jury or bench trial.

2. Pain Points in Determining Whether an Incident Is "Material"

Materiality assessments need to be adequately conducted, which can be tricky in any context. Remember, the new rule not only requires that material incidents be disclosed, but also that all material aspects or details of the incident are disclosed. Proper disclosure requires careful coordination between stakeholders and attorneys who are well versed in the SEC's "materiality" standard, as well as with frontline incident responders with a firm grasp of the evolving factual understanding of a given incident. Regulators view an organization as a holistic unit, and expect such collaboration to be effective, even though the reality is that a significant amount of information can be lost in translation.

An SEC enforcement action related to a failure in First American Financial Corporation's (First American) disclosure controls and procedures helps to illustrate this point. In June 2021, the SEC issued a cease-and-desist order and levied a fine against First American for failing to properly assess the quality of its disclosure relating to a cybersecurity incident. The core of the allegations relate to a failure in First American's process for assessing the need for a cybersecurity incident-related disclosure, as opposed to the ultimate content of their disclosure. The incident itself involved First American's "EaglePro" application, which was used to share document images related to title and escrow transactions. The EaglePro application lacked any real form of security since 2003 over a subset of documents stored there. For these documents, many containing sensitive financial information, the only "security" applied was the use of URLs that included a sequentially assigned numerical code that would increase by one for every new document stored in the application. This would mean that anyone that had one of these URLs could simply change the associated number and see someone else's closing documents. While this vulnerability had existed since 2003, a cybersecurity journalist disclosed the vulnerability to First American on May 24, 2019. First American filed a Form 8-K four days later, with the following description: "First American Financial Corporation advises that it shut down external access to a production environment with a reported design defect that created the potential for unauthorized access to customer data."

You may be asking yourself, if First American disclosed the incident, what could possibly be the problem? The SEC noted that First American personnel had discovered this vulnerability back in January of 2019, and even scheduled its remediation pursuant to its own vulnerability management policy. However, for whatever reason, that remediation was never completed. The SEC's stated concern was that the senior executives responsible for filing the Form 8-K statement describing the incident "lacked certain information to fully evaluate the company's cybersecurity responsiveness and the magnitude of the risk from the … vulnerability at the time they approved the company's disclosures." In other words, the SEC had certain expectations as to how in-depth, and effective, diligence surrounding a disclosure statement needed to be, and found First American's process here lacking. What was missing was an assessment of the fact that the vulnerability had been known to the company for approximately five months prior to the incident, but it had not remediated the known issue in violation of its own policies. While the SEC did not go as far as saying that this fact needed to be in the Form 8-K disclosure, it did make clear that it was a violation for the senior executives responsible for drafting the disclosure to not have been aware of that fact.

Accordingly, it is crucially important for businesses to put in place sufficient processes to ensure that 1) potentially material incidents are assessed by legal counsel, and 2) that counsel can engage with the investigation beyond a summary of findings to date, in an effort to identify all of the ways it can later be viewed as "material."

Practical Tips

1. **Identify, assess, and manage all your representations about security.** As noted above, the delta between what your organization represents about its security, and what an incident says about that representation, is one of the ways that an incident can be considered "material." This is true even where an incident responder might not have considered the incident "significant." That potential delta can be narrowed or closed without running afoul of the new disclosure rules by managing the affirmative representations your organization is making in its public filings and marketing statements.

2. **Understand the "materiality" implications of your organization's internal escalation processes.** These likely include escalation protocols that might actually use the term "material" or otherwise leverage proxies for materiality (e.g., significant reputational harm, impact to a threshold number of accounts, disruption of operations for a certain amount of time). If, for example, your information security stack leverages incident severity labels such as P0 - P5 alerts, it is important to engage experienced legal counsel to review such severity labels and assess how well they conform to a materiality assessment. The next step is ensuring that the right

resources and escalations are in place for a timely materiality assessment by the appropriate resources, in a manner that aligns to these classifications. This may mean not only reviewing your organization's incident severity framework, but also its incident response processes and relevant "RACI" charts identifying who is responsible, accountable, consulted, and informed of particular events.

3. **Understand how much your particular organization's business model implicates a greater reliance on good cybersecurity.** As noted above, materiality is all about the perspective of the reasonable investor. Setting aside any affirmative representations your organization may have made, it can be helpful to assess how unusually important cybersecurity is to your organization's business model. Because materiality is focused on the expectations of the reasonable investors, it can be helpful to assess whether there is reason for investors to have heightened expectations with respect to the security of your organization's network.

4. **Make sure that legal determinations are not being pushed down to your organization's technical staff.** Ask any securities lawyer what "materiality" means in the context of SEC disclosure requirements, and they will respond that information is material where there is substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the "total mix" of information made available. That articulation is not a standard technical folks should be expected to apply and should be translated to organizationally specific metrics that can act as a proxy for a potentially material event. As noted in the guidance, organizations need to take a broad view as to what may be material. This means if an organization is doing things correctly, the company's legal resources assessing materiality may often assess many cyber incidents that end up not being material. If everything that they assess ends up being material, this is an indication that the organization's escalation processes are likely missing potentially material incidents for consideration.

This blog has been republished in *Insights, The Corporate & Securities Law Advisor*.

Authors

Explore more in

Privacy & Security Data Security Counseling and Breach Response