Speech

Cybersecurity Disclosure

Erik Gerding
Director, Division of Corporation Finance

Dec. 14, 2023

As is customary, I am expressing my views today in my official capacity as Director of the SEC's Division of Corporation Finance, and my views do not necessarily reflect the views of the Commission, any of the Commissioners, or any other Commission staff.

In July of this year, the Commission adopted final rules that will require public companies to disclose both material cybersecurity incidents they experience and, on an annual basis, material information regarding their cybersecurity risk management, strategy, and governance.[1] These rules will provide investors with timely, consistent, and comparable information about an important set of risks that can cause significant losses to public companies and their investors. This disclosure can help investors evaluate those risks as they make investment and voting decisions.

In recommending these final rules, the staff of the Division of Corporation Finance, together with staff from around the Commission, carefully considered the comments the Commission received[2] on the March 2022 proposed rules.[3] The Commission took these comments—including concerns about compliance and threat actors—into account in deciding to make changes from the proposal and in fashioning a set of rules that advance our goals of protecting investors and facilitating capital formation.

Because some of the new disclosure requirements will take effect later this month, it is important to underscore the changes the Commission made from the proposal, highlight some significant parts of the rationale and mechanics of these rules, and clear up potential misconceptions.

1. Overview of the Rule and Its Rationale

The Commission and its staff have been addressing cybersecurity risk disclosures for many years. In 2011, the staff—and in 2018, the Commission itself—issued guidance on how existing disclosure rules apply to cybersecurity risks and incidents. Although public companies' disclosures of material cybersecurity incidents and cybersecurity risk management and governance improved since that guidance was issued, disclosure practices have remained inconsistent. Thus, the Commission determined that new rules would provide investors with the more timely, consistent, comparable, and decision-useful information they need to make informed investment and voting decisions.

The Commission has noted that cybersecurity risks have increased alongside the ever-increasing share of economic activity that depends on electronic systems, the growth of remote work, the ability of criminals to monetize cybersecurity incidents, the use of digital payments, and the increasing reliance on third party service providers for information technology services, including cloud computing technology. In my view, artificial intelligence and other technologies may enhance both the ability of public companies to defend against cybersecurity threats but also the capacity of threat actors to launch sophisticated attacks. The Commission also

observed that the cost to companies and their investors of cybersecurity incidents is rising at an increasing rate. All of these trends highlight investors' need for improved disclosure.

The final rules meet this need. At the same time, it is important to underscore what these rules do not do in order to address a potential misconception. The Commission is not seeking to prescribe particular cybersecurity defenses, practices, technologies, risk management, governance, or strategy. Public companies have the flexibility to decide how to address cybersecurity risks and threats based on their own particular facts and circumstances. Investors have indicated, however, that they need consistent and comparable disclosures in order to evaluate how successfully public companies are doing so.

To help investors evaluate this, the final rule has two components: a requirement to disclose material cybersecurity incidents four business days after a public company determines the incident is material and a requirement to disclose annually information regarding cybersecurity risk management, strategy, and governance. I'll discuss each of these requirements in turn.

2. The Cybersecurity Incident Disclosure Provision

To understand the cybersecurity incident disclosure requirement, it is helpful to ask and answer three questions: what must be disclosed, when must that information be disclosed, and why did the Commission use a materiality standard.

What must be disclosed? The final rule requires public companies to disclose the occurrence of a material cybersecurity incident and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations. This disclosure is focused on the material impacts of a material cybersecurity incident. It is narrower than what the Commission originally proposed, which would have required additional details that were not explicitly limited by materiality. In revising the disclosure requirement, the Commission took into account not only the company's compliance costs but also its need to respond and remediate incidents. The final rule contains an instruction stating:

A registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident.[4]

The Commission thus balanced the need for disclosure with the risk that disclosing specific technical information could provide a road map that threat actors could exploit for future attacks.

When must it be disclosed? Public companies must provide the required cybersecurity incident disclosure within four business days after the company determines the incident to be material. The deadline is *not* four business days after the incident occurred or is discovered. This timing recognizes that, in many cases, a company will be unable to determine materiality the same day the incident is discovered. A public company may alert similarly situated companies as well as government actors at any point in its incident response, including immediately after discovering an incident and before determining materiality, so long as it does not unreasonably delay its internal processes for determining materiality. The Commission had proposed a "as soon as reasonably practicable" standard but changed this to requiring a materiality determination for a cybersecurity incident "without unreasonable delay." The "without unreasonable delay" standard in the final rule was intended to address commenter concerns regarding the timing of the materiality determination. As the Commission recognized in the adopting release, "a materiality determination necessitates an informed and deliberative process."[5]

Some have asked why the Commission chose four business days as the deadline for disclosure. This timing is consistent with the reporting of other events the Commission requires be reported on a Form 8-K, such as entry into or termination of a definitive material agreement or a bankruptcy. In adopting the four business-day deadline, the Commission explained that cybersecurity incident disclosure was not sufficiently different from other Form 8-K reporting events to warrant a different approach.

The Commission also recognized that a company may not have complete information about the incident even if it knows enough to determine the incident was material. If the company does not know all the information required to be disclosed four business days after a materiality determination, the final rule contains a mechanism for the company to disclose that information in a subsequent filing.[6]

Why use a materiality standard? I also have heard some people, perhaps less familiar with the Federal securities laws, asking why the standard for disclosure here is limited to "material" cybersecurity incidents. Some seem to prefer a more bright line rule. Materiality is a touchstone of securities laws. It connects disclosures back to the needs of investors. I don't mean to suggest that all disclosures required under the Federal securities laws have or must have a materiality qualifier. Some required disclosures do not.[7] In this case, the Commission determined that a materiality qualifier was appropriate. In my view, this makes sense when you consider that some companies may experience cyber attacks on a daily basis if not more frequently.

In both the adopting release and the proposing release,[8] the Commission affirmed that the materiality standard companies should apply for the cybersecurity incident disclosure is the same standard articulated by the Supreme Court in cases such as *TSC Industries, Inc. v. Northway*,[9] *Basic, Inc. v. Levinson*,[10] and *Matrixx Initiatives, Inc. v. Siracusano*,[11] as well as in Commission rules.[12] The Commission declined to adopt a new standard for materiality unique to cybersecurity. Using this time-tested and familiar materiality standard, rather than a new bespoke standard, is consistent with the overarching rationale for the rule: to give investors disclosure to help assess risks to their investments, in the same way that they receive consistent and comparable disclosure about other risks that public companies face.

3. The National Security and Public Safety Delay Provision

In the final rule, the Commission also provided for delayed reporting of cybersecurity incident disclosures that would pose a substantial risk to national security or public safety, contingent on a written notification by the Attorney General, who may take into consideration other Federal or other law enforcement agencies' findings. The Commission adopted this provision in response to comments received on the proposed rule. I note that the Department of Justice (DOJ) recently issued guidelines describing the process a company should follow to obtain a delay and the procedures the Attorney General will use to evaluate whether a delay is warranted.[13] According to the DOJ guidelines, Federal Bureau of Investigation (FBI) field offices will be the primary points of contact for companies that have experienced cybersecurity incidents.[14]

Earlier this week, the Division of Corporation Finance also issued a Compliance & Disclosure Interpretation (CDI) to clarify whether companies consulting with the DOJ, which includes the FBI, the Cybersecurity & Infrastructure Security Agency (CISA), and any other law enforcement or national security agency about a cybersecurity incident automatically means that that incident must be material.[15] This C&DI reads as follows:

> Question: Would the sole fact that a registrant consults with the Department of Justice regarding the availability of a delay under Item 1.05(c) necessarily result in the determination that the incident is material and therefore subject to the requirements of Item 1.05(a)?
>
> Answer: No. As the Commission stated in the adopting release, the determination of whether an incident is material is based on all relevant facts and circumstances surrounding the incident, including both quantitative and qualitative factors, and should focus on the traditional notion of materiality as articulated by the Supreme Court.
>
> Furthermore, the requirements of Item 1.05 do not preclude a registrant from consulting with the Department of Justice, including the FBI, the Cybersecurity & Infrastructure Security Agency, or any other law enforcement or national security agency at any point regarding the incident, including before a materiality assessment is completed.

I hope this underscores that the rule does not create a disincentive for public companies to consult with law enforcement or national security agencies about cybersecurity incidents. Indeed, I would encourage public

companies to work with the FBI, CISA, and other law enforcement and national security agencies at the earliest possible moment after cybersecurity incidents occur. I believe this timely engagement is in the interest of investors and the public. While this is not within the Commission staff's purview, companies and government agencies may find that such timely engagement could assist them in a later determination of whether to seek a delay from the DOJ.

Consultations with national security and law enforcement agencies may, of course, help companies to better understand the impact or severity of a particular incident and thus to assess whether the incident is material. But ultimately it is the company's responsibility to make a materiality determination based on a consideration of all relevant facts and circumstances. In this regard, it's worth bearing in mind that the analyses of cybersecurity incidents by these other agencies may take into account factors other than a focus on a reasonable investor. This is consistent with the CDI above. And, as I noted previously, the Commission did not establish a fixed timeline for making a materiality determination, and a company's consultation with any national security or law enforcement does not change this and start the clock on a fixed timeline with respect to a cybersecurity incident. Again, instead of a fixed timeline, the Commission included Instruction 1 to Item 1.05, which states that "[a] registrant's materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident."[16]

4. The Risk Management, Strategy, and Governance Disclosure Provisions

The rule also requires public companies to make annual disclosures about their cybersecurity risk management, strategy, and governance. Recognizing commenter concerns, the Commission streamlined the required disclosures, as compared to the proposal, to avoid being overly prescriptive or empowering threat actors to the detriment of companies and their investors.

For example, in the final rule, the Commission removed a proposed requirement that public companies disclose whether any members of their board have cybersecurity expertise. Commenters expressed concerns that the proposal might inadvertently pressure companies to retain an expert on the board, and that investment in such an expert could come at the expense of other investments in cybersecurity or other priorities for board oversight. Instead, the final rule focuses on disclosures regarding management's role in assessing and managing material risks from cybersecurity threats, including, as applicable, whether and which management positions or committees are responsible for cybersecurity threats, and their relevant expertise. The final rule's disclosure requirement regarding the board, by contrast, is more high level, focused on describing the board's oversight of risks from cybersecurity threats, and, if applicable, identifying any relevant board committee or subcommittee and describing how the board or such committee is informed of such risks.

Likewise, whereas the proposal would have required disclosure regarding a public company's cybersecurity policies and procedures as well as certain specific details regarding those policies and procedures, the final rule focuses more broadly on the company's cybersecurity processes, if any, and includes a non-exclusive list of disclosure items. This formulation recognizes that companies will have diverse approaches to cybersecurity, based on their particular circumstances, and that not every company needs formal policies and procedures.

5. Next Steps

As the final rules begin to take effect, we recognize that public companies will be working to ensure compliance with them. This might involve fostering conversations among chief information security officers, a company's other cybersecurity experts and technologists, the company's disclosure committee, and those responsible for advising them on securities law compliance. As interpretative questions arise, I would like to emphasize the Division's longstanding open door policy. Come talk to staff about your questions. We recognize that the disclosure belongs to public companies and that public companies and their advisers are on the front line of disclosure and informing investors.

The Commission staff are busy at work too. We are working not just to answer questions and explain the rule, but also to prepare the attorneys and accountants in our Disclosure Review Program to review disclosures. For our Disclosure Review Program, the first year of a rule is very important. But I want to reassure companies and their representatives that our Division does not seek to make "gotcha" comments or penalize foot faults. To the extent appropriate, we may issue forward-looking comments to companies or additional CDIs. This is a similar message to one I and others at the Division have given with respect to other disclosure rules that have recently gone into effect, such as the Pay versus Performance rules.[17] I recognize the value of creating incentives for good faith efforts to comply with new rules, and I hope this message and our Division's track record with respect to those other rules provides reassurance to companies and their advisers, particularly in the first year of effectiveness for this rule.

In recommending new disclosure requirements to the Commission, our goal as staff is not simply to have another rule on the books, to simply add to a company's compliance "checklist," or to induce boilerplate disclosures. Rather, we are hoping to elicit tailored disclosures that provide consistent, comparable, and decision-useful information to investors, in this case about risks that didn't really exist (or at least didn't exist in the current form and to the current extent) when I began practicing as a lawyer several decades ago. Even when a risk is emergent or evolving, disclosure rules can provide the same benefits in terms of investor protection and capital formation that they have for risks that public companies have faced for decades.

---

[1] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release Nos. 33-11216; 34-97989 (July 26, 2023) [88 FR 51896 (Aug. 4, 2023)] ("Adopting Release").

[2] The public comments the Commission received on the proposed rules are available at https://www.sec.gov/comments/s7-09-22/s70922.htm.

[3] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release No. 33-11038 (Mar. 9, 2022) [87 FR 16590 (Mar. 23, 2022)] ("Proposing Release").

[4] Instruction 4 to Item 1.05 of Form 8-K.

[5] Adopting Release at 51906.

[6] *See* Instruction 2 to Item 1.05 of Form 8-K ("To the extent that the information called for in Item 1.05(a) is not determined or is unavailable at the time of the required filing, the registrant shall include a statement to this effect in the filing and then must file an amendment to its Form 8–K filing under this Item 1.05 containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available.").

[7] *See, e.g.*, 17 CFR 229.402(a)(2) (requiring "disclosure of all plan and non-plan compensation awarded to, earned by, or paid to" certain executive officers and directors).

[8] *See* Adopting Release at 51899-900; Proposing Release at 16596.

[9] 426 U.S. 438, 449 (1976).

[10] 485 U.S. 224, 232 (1988).

[11] 563 U.S. 27 (2011).

[12] *See* 17 CFR 230.405; 17 CFR 240.12b-2.

[13] *See* Department of Justice Material Cybersecurity Incident Delay Determinations (Dec. 12, 2023), *available at* https://www.justice.gov/media/1328226/dl?inline.

[14] *See id.* at 2 (“When a registrant discovers a cybersecurity incident and believes that disclosure may pose a substantial risk to national security or public safety, the registrant should, directly or through another U.S. Government agency (*e.g.*, the U.S. Secret Service, another federal law enforcement agency, the Cybersecurity & Infrastructure Security Agency (CISA), or another sector risk management agency (SRMA)), immediately contact the FBI consistent with reporting instructions the FBI has issued.”). The FBI’s reporting instructions are available at https://www.fbi.gov/investigate/cyber/fbi-guidance-to-victims-of-cyber-incidents-on-sec-reporting-requirements.

[15] *See* Exchange Act Form 8-K Compliance and Disclosure Interpretations, Questions 104B.01, 104B.02, 104B.03, and 104B.04, *available at* https://www.sec.gov/divisions/corpfin/guidance/8-kinterp.htm.

[16] *See* Instruction 1 to Item 1.05 of Form 8-K (“A registrant’s materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident.”).

[17] *See* Pay Versus Performance, Release No. 34-95607 (Aug. 25, 2022) [87 FR 55134 (Sep. 8, 2022)].