NOW & NEXT

Public Finance Alert

APRIL 11, 2022

What should the municipal securities market learn from the SEC's recent proposed corporate cybersecurity rules?

By Elizabeth M. Columbo, Daniel M. Deaton, and Mitchell Rapaport

Municipal market participants may find the SEC's proposed rules to be helpful in crafting their own cybersecurity disclosure.

What's the Impact?

- The proposed rules would clarify the SEC's views on the necessity and materiality of cybersecurity disclosure, which can be helpful to both the municipal securities and corporate securities markets
- The proposed rules can guide the municipal securities market in determining whether disclosure is necessary and in crafting such disclosure

On March 9, 2022, the United States Securities and Exchange Commission (SEC) proposed sweeping changes to the corporate securities disclosure rules that would require corporate issuers of stock and debt securities to make new disclosures concerning cybersecurity risks and incidents.[1] The proposed rules do not apply to municipal securities market. However, while the proposed rules only apply to corporate issuers, municipal market participants may find the SEC's

[1] Release Nos. 33-11042; 34-94478.

commentary to be helpful in applying the disclosure requirements that apply to them. In the release for the proposed rules, the SEC provided commentary concerning the necessity for the proposed rules and how public companies should approach compliance with the proposed rules if approved. This commentary sheds light on the SEC's views on the necessity and materiality of cybersecurity disclosure under the proposed rules, all of which can be as helpful to the municipal securities market as to the corporate securities market.

What are the SEC's proposed rules for Cybersecurity Disclosures?

The SEC's proposed rules require two new kinds of cybersecurity disclosures:

- Public companies will be required to disclose any material cybersecurity incident within four business days after it determines that it has experienced such an incident; and
- Public companies will be required to include new categories of information in their periodic disclosures, including (1) a description of their policies and procedures to identify and manage cybersecurity risks, (2) management's role in implementing cybersecurity policies and procedures, and (3) board of director's cybersecurity expertise and oversight of cybersecurity risk.

What we found interesting about the SEC's proposed rules

In our review of the SEC's proposed rules, we found that the SEC provided valuable guidance that can be just as applicable to disclosure in the municipal securities market as it is for public companies. Here are some of our observations:

The SEC provided insight concerning what may be wrong with current cybersecurity disclosure.

The SEC's major concern about current public company cybersecurity disclosure appears to be the lack of a systematic approach both by public companies as a whole and by specific public companies. The SEC stated that "companies provide different levels of specificity regarding the cause, scope, impact, and materiality of cybersecurity incidents." In addition, the SEC cited a report that "noted a disconnect in which the industries experiencing the highest profile cybersecurity incidents provided disclosure with the 'least amount of information.'" Further, the SEC stated that it sought to enhance cybersecurity disclosures to provide more information about incidents and provide information concerning policies and procedures and risk management. In proposing these rules, it does not appear that the SEC was focused on criticizing existing disclosure practices by public companies but rather was addressing a need for public companies to more systematically and consistently provide a wider array of information concerning cybersecurity risks, incidents, and practices to better inform investors.

The SEC provides helpful guidance concerning when cybersecurity incidents are material.

In the release, the SEC provided guidance concerning how public companies should evaluate whether an incident is material in determining whether they are required to provide disclosure about the incident within four business days. While municipal issuers are not subject to that

notification requirement, municipal issuers can still learn from the SEC's discussion of what it considers to be a material cybersecurity incident. After stating that the materiality analysis should be no different for these purposes than any other materiality disclosure question, the SEC stated the following:

> A materiality analysis is not a mechanical exercise, nor should it be based solely on a quantitative analysis of a cybersecurity incident. Rather, registrants would need to thoroughly and objectively evaluate the total mix of information, taking into consideration all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors, to determine whether the incident is material. Even if the probability of an adverse consequence is relatively low, if the magnitude of the loss or liability is high, the incident may still be material; materiality "depends on the significance the reasonable investor would place on" the information.

In other words, the SEC applied the same legal standard that is used any time that an issuer applies the materiality standard to a securities disclosure. But what was particularly helpful was that, in addition to this general materiality guidance, the SEC provided specific examples (which it referred to as a "non-exhaustive list") of cybersecurity incidents that may trigger required disclosure for a public company:

- An unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset (data, system, or network); or violated the registrant's security policies or procedures. Incidents may stem from the accidental exposure of data or from a deliberate attack to steal or alter data;
- An unauthorized incident that caused degradation, interruption, loss of control, damage to, or loss of operational technology systems;
- An incident in which an unauthorized party accessed, or a party exceeded authorized access, and altered, or has stolen sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the registrant;
- An incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; or
- An incident in which a malicious actor has demanded payment to restore company data that was stolen or altered.

Taken together, the SEC provides some insight into what it considers material cybersecurity incidents and material cybersecurity disclosure as a whole, which can then in turn help issuers of municipal securities to determine whether disclosure is necessary and, if so, to craft their own disclosure. The SEC's non-exhaustive examples target either (a) significant unauthorized parties accessing information, operational technology systems or sensitive business information that either calls into question the integrity of the public company's systems or policies and procedures, or has created loss or liability or (b) a malicious actor is threatening to hurt the public

company by disclosing sensitive information or blocking the public company from its data. The SEC is focused on cybersecurity risks that create risk for the operational integrity of the public company or risks that present potential for enough loss or liability that it can affect investments in the public company.

The SEC focuses as much on risk management, strategy, and governance as it does on incidents.

The SEC stated that "[s]taff in the Division of Corporation Finance has observed that most of the registrants that disclosed a cybersecurity incident in 2021 did not describe their cybersecurity risk oversight and related policies and procedures." The SEC stated that it believes that this information benefits investors for two reasons. First, disclosure about a cybersecurity risk assessment program and related activities designed to prevent, detect, and minimize effects of cybersecurity incidents can improve an investor's understanding of the company's risk profile. Second, cybersecurity risks can affect different businesses differently and accordingly can impact the business strategy of the company. The SEC cited examples of how cybersecurity risks can impact business strategy. A company that knows it relies on collecting and safeguarding sensitive and personally identifiable information from its customers may need to raise capital to improve its technological ability to protect that information. Also, a company may develop a business model that avoids collecting this information. In each case, these "strategic decisions have implications for the company's financial planning and future financial performance." Thus, in short, the SEC believes that disclosure concerning how management of a company perceives a cybersecurity risk and what the company plans on doing about that risk are important disclosures to investors that form a critical part of the cybersecurity profile of the company.

The SEC discussed its concern of cybersecurity incidents that are material in the aggregate.

One of the new disclosures that would become required if the proposed rules are approved would be to disclose when a series of previously undisclosed, individually immaterial cybersecurity incidents become material in the aggregate. The SEC explains as follows: "While such incidents conceptually could take a variety of forms, an example would be where one malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material, or both." While the SEC does not say this, presumably one factor in such a series of incidents is that in the aggregate it may paint a picture of a lack of technological integrity that is, in that light, material.

The SEC provides some valuable definitions.

The SEC provides valuable definitions of "cybersecurity incident," "cybersecurity threat," and "information systems" that municipal securities market participants may find helpful in defining what constitutes cybersecurity events that may require disclosure. Here is how the SEC defined these terms:

- Cybersecurity incident means an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality,

integrity, or availability of a registrant's information systems or any information residing therein.

- Cybersecurity threat means any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.
- Information systems means information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

What should municipal market participants take away from this?

We believe that there are a number of principles that the municipal securities market can glean from the proposed rules in determining whether disclosure is necessary and in crafting disclosure. For the municipal securities market, the guidance must be considered both in the context of complying with the requirement to disclose material issues in their offering documents as well as whether subsequent disclosures should be made (even if not specifically required by Rule 15c2-12).

First, the SEC focused on the perspective of an investor—both in terms of what disclosure is material as well as making sure investors have the information they need to make good investment decisions.

Second, every municipal issuer, like every public company, is different. Some municipal issuers may be natural targets for malicious actors or have operational vulnerabilities that can be susceptible to unauthorized access. The SEC appeared to fashion the proposed rules to drive public companies to take a long, hard look at their own circumstances and consider whether they have appropriately disclosed all of their cybersecurity risks, incidents, or practices that may impact investors. While municipal market participants will not be subject to these rules if finalized, that is a step in preparing disclosure that would make sense for municipal securities market participants to adopt.

Third, much of the import of the proposed rules is to ensure, as in so many other areas of disclosure, investors have the benefit of the perspective of a company's management. In many parts of the rules, the SEC was not focused on cybersecurity risk, as such, but how management plans on addressing that risk and what is its strategy to address that risk. The SEC seemed to be just as concerned with cybersecurity risk as with how a public company is planning to react to those risks. Its example of a company raising capital to address known vulnerabilities is a good one. The SEC appeared to be trying to broaden the focus of cybersecurity disclosure and recognizing that what management knows about current cybersecurity risk and how that risk may inform future planning, strategy, and governance approaches may ultimately impact investors more than the risk itself.

Fourth, while the proposed requirement to provide notice of material cybersecurity incidents within four business days does not apply to the municipal securities market, it should at least give the municipal securities market pause to consider whether there are some cybersecurity incidents that are significant enough to warrant making a voluntary disclosure to investors. This may also be the case if investors become accustomed to regular incident notices in the corporate securities market from public companies and expect the municipal securities market to do the same.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Elizabeth M. Columbo
212.940.3183
ecolumbo@nixonpeabody.com

Daniel M. Deaton
213.629.6050
ddeaton@nixonpeabody.com

Mitchell Rapaport
202.585.8305
mrapaport@nixonpeabody.com