BRACEWELL

Cybersecurity Disclosure Considerations for Municipal Issuers

Article

March 14, 2024 | *The Bond Buyer* | 2 minute read

In the Closing Remarks of a Compliance Conference on December 7, 2023, the Director of the Office of Municipal Securities of the US Securities and Exchange Commission noted the SEC recently finalized its cybersecurity rule for public companies. The Director then suggested that "everyone take a minute to review the Adopting Release for the rule because there are some good points on how corporations can handle cybersecurity disclosures that may be useful for municipal market participants."

While the Commission's cybersecurity rule does not apply to municipal issuers, below we summarize a few points discussed in the Adopting Release that may be useful for municipal market participants.

If a municipal issuer chooses to voluntarily disclose a material cybersecurity incident, it should consider various factors.

First, the municipal issuer should consider disclosing the nature, scope, and timing of the material cybersecurity incident. Municipal issuers should avoid specific or technical information about a planned response to the incident, its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail that it would impede a response or remediation of the incident.

Second, the municipal issuer should consider disclosing the material impact or reasonably likely material impact of the incident (e.g., impact on the financial condition or operations of the municipal issuer), as opposed to the details regarding the incident itself.

Related People

Edward Fierro
Partner
HOUSTON
+1.713.221.1107
ed.fierro@bracewell.com

Sarah Tahir
Associate
DALLAS
+1.214.758.1047
sarah.tahir@bracewell.com

Related Industries

Energy

Technology

Related Practices

Public Finance

Third, the municipal issuer should consider timing of any voluntarily disclosure. Municipal issuers should consider disclosing after it determines the incident is material, as opposed to immediately after the incident occurred.

Fourth, the materiality determination of the incident should be made without unreasonable delay. That said, a reasonable delay could occur, for example, if an incident poses a substantial risk to national security or public safety.

Lastly, the materiality analysis should take into consideration all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors. The materiality standard is the traditional notion of materiality that has been articulated by the Supreme Court, as well as in Commission rules (e.g., information is material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision).

If a municipal issuer chooses to disclose cybersecurity information in connection with an offering, it should consider disclosing certain matters.

First, the municipal issuer should consider disclosing the process that it may have for assessing, identifying and managing material risk from cybersecurity threats, as opposed to the specifics on how a cyberattack will be remediated.

Second, the municipal issuer should consider disclosing risks from cybersecurity threats, including those resulting from previous incidents, that may have materially affected or are reasonably likely to materially affect the municipal issuer (e.g., operations or financial condition).

Lastly, the municipal issuer should consider whether to disclose consultants or other third parties that may assist with cybersecurity and who is responsible for oversight of risks from cybersecurity threats.

Any cybersecurity disclosure should allow for a reasonable investor to ascertain the cybersecurity practices of the municipal issuer with sufficient detail to understand the municipal issuer's cybersecurity risk profile. Municipal issuers should tailor disclosures so that they provide meaningful cybersecurity information, as opposed to overly descriptive or boilerplate disclosure.

The SEC recognizes that public companies will have differing approaches to cybersecurity disclosure based on their particular facts and circumstances. We hope such recognition will also extend to municipal issuers.

Article originally published by The Bond Buyer on March 14, 2024.