The Financial and Regulatory Impact of Cyberattacks on Municipal Bond Issuers

Sep 09, 2026

Categories:

Matters of Interest
Publications

Authors:

Allie Butchello
Emmett M. Kelly

Almost two years ago, the Township of White Lake, Michigan experienced a cyberattack while closing on the issuance of $29 million in general obligation bonds to finance new government buildings. The hackers were able to gain access to the township's email system, impersonate a government official, and send altered wire instructions to the underwriter of the bond. The attack led to the issuance being canceled, and the underwriter sued the township.

In a separate incident last year, municipal-bond offering distribution platform MuniOS was taken out of service for several days following a cyberattack. While this incident did not appear to cause delays in any deals, it required issuers to adjust to using different platforms and served as a reminder that the municipal market's digital infrastructure itself is a target.

These are not isolated incidents. Cyberattacks are a daily threat, and White Lake is not the only local government to fall victim. Ransomware attacks against state and local governments have increased steadily year over year and are using increasingly more sophisticated schemes.

Financial and Credit Consequences

Cyberattacks can be costly to local governments beyond diverted funds. Remediation and litigation can impose significant costs on local governments that are already working with limited resources.

Research has shown that following a data breach, bond prices of the target issuer in the secondary market decline, indicating that investors demand a discount to hold the bonds of an entity that has suffered a breach.

Credit rating agencies have started to incorporate cybersecurity attack preparedness into overall risk assessments, treating cyber

FBT Gibbons

resilience as a component of risk profiles. Moody's, S&P, and Fitch have each identified cybersecurity as a credit factor, particularly for issuers in critical infrastructure industries such as energy, healthcare, and government services. Cyber insurance coverage is becoming harder to qualify for, with underwriters demanding more evidence of strong cybersecurity.

Rating agencies have begun downgrading credit following cyberattacks. In California, Palomar Health saw its credit rating downgraded by Fitch twice over a matter of months following pressured financial performance that was exacerbated by a significant cyber event with a months-long recovery. Frederick Health in Maryland experienced a similar downgrade. These actions signal that agencies are no longer treating cyber events as one-time operational disruptions but as indicators of broader governance weaknesses that can have lasting credit implications.

Regulatory Landscape: Movement at the State Level

There have been few regulatory changes at the federal level in recent years, despite continued threats and mounting calls for guidance. The Securities and Exchange Commission (SEC) has issued requirements for public companies to quickly disclose material cyber incidents and report annually on cybersecurity risk management. However, the SEC has not issued municipal-market-specific cybersecurity rules, and the MRSB has limited its engagement to largely educational resources and best practice recommendations.

In response to increased cybersecurity incidents involving public-sector entities, Ohio Governor Mike DeWine signed Ohio House Bill 96 on June 30, 2025, which became effective on September 30, 2025. The new Ohio Revised Code (ORC) Section 9.64 applies to all political subdivisions, including counties, townships, municipal corporations, and school districts. Under the law, every political subdivision is required to adopt a cybersecurity program to safeguard data, IT, and IT resources to ensure availability, confidentiality, and integrity.

ORC Section 9.64 also generally prohibits political subdivisions experiencing ransomware incidents from paying or complying with a ransom demand and adds a reporting requirement to the Ohio Department of Public Safety's Division of Homeland Security and the Auditor of State. This prohibition aligns Ohio with a growing number of jurisdictions that have concluded that paying a ransom funds criminal enterprises and incentivizes further attacks.

Ohio is not alone, joining an increasing number of states that have enacted or proposed cybersecurity mandates for public entities in recent years. For example, Texas requires local governments to report cyber incidents to the state's Department of Information Resources within 48 hours of discovery. While these state-level frameworks are promising, they vary in scope and enforcement, creating a patchwork of requirements across jurisdictions.

Bond Market Implications

A gap remains in the broader municipal bond market, and the threat of cyberattacks is not going away.

For issuers, the message is clear: cybersecurity preparedness is not optional and is no longer solely an IT concern. Issuers should evaluate whether their existing cybersecurity programs are adequate and whether they carry appropriate cyber insurance.

For underwriters and bond counsel, the White Lake incident highlights the need for enhanced closing procedures, including multi-factor authentication for instructions, callback verification protocols, and clear policies for identifying and responding to suspicious communications during the deal process. End-to-end encryption of emails should also be considered to make exchanges harder to intercept, disrupt, or otherwise compromise.

Looking Ahead

The municipal bond market's vulnerability to cyberattacks is likely to grow as local governments continue to digitize operations, adopt cloud-based platforms, and rely on interconnected vendor networks. At the same time, threat actors are becoming more sophisticated.

FBT Gibbons

Until a more comprehensive framework emerges, market participants should treat cybersecurity as a present and material risk factor. The costs of inaction, measured in diverted funds, downgraded credit, and higher borrowing costs, will only continue to mount.

For further guidance on how evolving cybersecurity threats and state-level requirements may affect your next issuance, please contact the author or any member of our Public Finance team.

FBT Gibbons