Bond Case Briefs

Municipal Finance Law Since 1971

Add Cyberattacks to the List of Municipal Bond Credit Risks.

- **Baltimore ransomware attacks underscore threat: Breckinridge**
- **More than 20 ransonware attacks on municipalities this year**

Huge pension debt. Crumbling infrastructure. Climate change. Now add cyberattacks to the list of things that municipal bond investors should worry about.

The recent ransomware attack that shut down some of Baltimore's computers, the second in 15 months, underscores the growing credit risk that cyberattacks pose to states and cities, according to Breckinridge Capital Advisors. The May 7 attack on Baltimore has hobbled the city's ability to collect water bills, property taxes, and parking revenue. It also shut down the city's system to process home sales. Baltimore's general obligation bonds, like much local debt, is payable by property taxes, which makes up about half of the city's revenue.

Cyberattacks also threaten to erode public confidence in government and can suggest weak governance, wrote Alriona Costigan, a vice president at Breckinridge and Jesse Starks, the firm's chief technology officer.

"Cyberattacks can hurt issuers' reputations, evidenced by the fact that many cities and states avoid reporting them," they wrote. "However, the lack of consistent reporting of cyberattacks could leave many issuers complacent about the risks or unaware of some of their own vulnerabilities."

This month's cyberattack in Baltimore follows last year's high profile ransomware attack in Atlanta, which cost the city an estimated $17 million to fix, about 2.6% of the city's budget, according to Boston-based Breckinridge, which oversees more than $37 billion in high-grade fixed income assets. There have been at least 24 reported ransomware attacks on municipalities this year, including Greenville, North Carolina, and 46 last year, according to Moody's Investors Service.

Smaller Targets

A study by the Massachusetts legislature reported 26 million attempts to access the state's computers in a one-hour period between 1 a.m. and 2 a.m. on Sept. 13, Breckinridge said.

In a ransomware attack, hackers infiltrate a computer system and deploy malicious software that locks a victim's data until the owner pays a ransom. Baltimore has refused to pay a ransom of around $100,000 worth of Bitcoins. The event is unlikely to have a material effect on the city's finances and Baltimore hasn't missed a debt service payment, Moody's said May 27.

Cyberattacks could have even more harmful affects on smaller state and local governments, which have less funding for cybersecurity and may see themselves as less of a target that big cities or states.

"Ransomware criminals may see smaller school districts or towns as easier targets, as their focus on cybersecurity is less than that of larger cities such as Los Angeles, which has a cybersecurity working group in place," Costigan and Starks wrote.

Investors need to determine whether states and local governments take cybersecurity seriously as a risk and issuers need to assess and share information about the defenses in place against cyberattacks, according to Breckinridge. Investors should also evaluate a municipality's preparedness for a cyberattack by evaluating whether they have a written response plan, the size of the cybersecurity budget and the presence of cyberinsurance.

"Even the most ironclad technological and physical defenses can be breached, so preparedness for cyberattacks is important to assess as a credit issue," Costigan and Starks wrote.

Bloomberg Cybersecurity

By Martin Z Braun

May 29, 2019, 10:29 AM PDT