# Bond Case Briefs

*Municipal Finance Law Since 1971*

---

## A Hidden Risk in the Municipal Bond Market: Hackers

**Cyberattacks leave schools, hospitals and utilities struggling to pay ransom, restore services and boost security**

Local governments are spending big to mop up after hacks and prevent new ones. That means peril—and opportunity—for the investors who buy their bonds.

Hacks are on the rise across all industries, but the public sector's weak protections make it an increasingly attractive target for cybercriminals. Cybercrime has left schools, hospitals and utilities from Baltimore to Los Angeles struggling to pay ransom, restore services and boost security. Finances have suffered, threatening credit ratings.

The number of K-12 public schools suffering ransomware attacks almost doubled between 2021 and 2022 to almost 2,000 a year, according to a report by Emsisoft, a cybersecurity company. The growing use of technology in education, which was accelerated by the Covid-19 pandemic, as well as healthcare's reliance on IT infrastructure, has made schools and hospitals particularly vulnerable, according to analysts.

"This year alone, we've seen a lot more of these attacks compared to prior years, and it's a concern that has come up in almost every discussion that we have with issuers," said Li Yang, lead analyst at S&P Global Ratings.

Cyberattacks on the Los Angeles Unified School District, the nation's second-largest school system, caused problems including the release of confidential student data. Superintendent Alberto M. Carvalho said officials convened a task force of cybersecurity experts to begin modernizing the district's technology. This year the school district sold hundred of millions of dollars of debt and plans to use $72 million to secure its technology infrastructure, according to a spokesperson.

So far, cyberattacks seem to act as a wake-up call for municipalities, leading to investments in security that reassure bondholders. Researchers at Massachusetts Institute of Technology found that following a ransomware attack, municipalities spent 50% more on technology and bond yields fell by 0.03 percentage point.

The Los Angeles Unified School District's renewed focus on cybersecurity attracted investors including Belle Haven Investments. Dora Lee, Belle Haven's director of research, said the firm views it as a boost for a borrower's creditworthiness when finance officials increase cybersecurity and the financial resources to weather an attack.

"Just as we evaluate whether or not a state or local government is continuing their investment in their physical infrastructure, we are also looking to see that continued investment in their IT software," Lee said.

No protocols govern disclosure about muni issuers' relative vulnerability to cyberattacks, ratings firms said. Downgrades would only come when the cleanup of a problem hurts the finances of the

local government.

That leaves investors scrambling to keep up. Big incidents, such as the one that crippled Baltimore's city government computers in 2019, attract notice. Less-prominent attacks don't always get the same attention.

"Markets are watching more closely, as big cyberattacks get big headlines, but smaller ones don't," said Daniel S. Solender, partner and director of tax-free fixed income at the asset manager Lord Abbett.

The Securities and Exchange Commission voted earlier this year to adopt rules requiring publicly traded companies to report cyberattacks. Starting later this month, companies will have to describe the processes under which they identify in their annual reports material cybersecurity risks.

Ratings firms are asking local governments issuing debt about the protections they have in place—such as whether they have cyber insurance and how quickly they are prepared to respond and recover in case of a cyberattack, said Rudy S. Salo, public-finance attorney and partner at Nixon Peabody.

"Cybersecurity has evolved as a risk factor, and starting in 2018, you started to see due diligence questions disclosed in bond deals, and two years later, more and more rating agencies took notice," said Salo.

Analysts expect the sophistication and frequency of cyberattacks will continue to evolve but worry that cyber risk management remains underfunded. There is cyber insurance available, but the costs can be prohibitively high for small government agencies. Job retention in information-technology departments is likely difficult when competing with the private sector, according to analysts.

Governments "don't usually run with much excess cash to plow into a state-of-the-art technology," said Lisa Washburn, managing director at Municipal Market Analytics, a bond research firm.

**The Wall Street Journal**

By Brenda León

Dec. 7, 2023