Bond Case Briefs

Municipal Finance Law Since 1971

S&P: U.S. Public Finance Issuers' Inconsistent Cyber Security Faces State-Backed Threats

Key Takeaways

- Sovereign-sponsored and politically motivated cyber attacks are targeting U.S. critical infrastructure, according to warnings by the U.S. Cybersecurity and Infrastructure Agency (CISA) and the FBI.
- Utilities' exposure to cyber risks are exacerbated by widespread failure to implement all federal cyber security standards. Smaller water systems appear particularly vulnerable, due to investment constraints, limited industry-level cooperation, and inconsistent application and quality of cyber risk oversight frameworks.
- Rated issuers in the transportation sector have a generally higher degree of cyber risk awareness, according to anecdotal evidence from meetings with management teams, though risk to fiscal health and operational services remains.

Foreign state-backed cyber attacks on U.S. infrastructure, including utilities and transport operators, continues to be a threat to both safety and critical services, according to warnings by U.S. security agencies including the Cybersecurity and Infrastructure Agency (CISA) and the FBI. At the same time, wide variations in the adoption and application of cyber security practices means many issuers, particularly among utilities, are failing to meet minimum federal standards aimed at preventing a breach by cyber criminals.

The targeting of U.S. public finance issuers, and the sector's cyber security preparations, were chief among the subjects discussed at S&P Global Ratings' recent U.S. Public Finance Credit Spotlight: The Changing Face Of Cyber Risk In U.S. Critical Infrastructure. The webinar also featured a fireside chat with Cyrus Bulsara, Chief Information Security Officer of Scripps Health.

Utilities' Varied Reponses
The potential for U.S. critical infrastructure providers to suffer disruption and damage by cyber criminals was highlighted by a May 2024 Environmental Protection Agency report, "Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities," which noted that about 70% of utilities inspected by federal officials over the last year were found to be in violation of standards intended to prevent cyber breaches. The prospect of a cyber incident at a water and sewage system supplier could be exacerbated by the absence of standard cyber security and hygiene guidelines that apply to operators.

"Smaller water systems were found to be particularly vulnerable," said Jenny Poree, S&P Global Ratings analyst and sector leader U.S. Water & Sewer Utilities." Moreover, the closing of those vulnerabilities faces myriad challenges including competing demands for financial and management resources, limited cooperation and sharing of resources by entities that have sophisticated cyber security operations, and weak or inconsistent cyber security frameworks."

The webinar also discussed the potential impact of prospective changes to staffing levels at

government agencies involved in cyber security and resilience, including CISA and the National Security Agency (NSA), and the potential for funding cuts to organizations including the Multi-State Information Sharing and Analysis Center (MS-ISAC).

Transportation: Providing A Path To Follow

On a more positive note, the webinar heard that transportation sector issuers rated by S&P Global Ratings generally demonstrate a high degree of cyber risk awareness. “We discuss in our management meetings and receive assurances from operators that they continue to embed cyber security into overall risk mitigation strategies and that these are reported to their governing boards,” said Kurt Forsgren, S&P Global Ratings analyst and sector leader U.S. Transportation.

The webinar participants agreed that cyber criminality is evolving and often innovating, though incidents were often traceable to well-understood but difficult to manage vulnerabilities, including hacks that leverage social engineering and third-party vendors. And there was consensus that issuers’ best defense against cyber criminality remains pro-active cyber risk management, including the enforcement of plans and protocols that reinforce good cyber hygiene and the purchase of cyber insurance.

29 May, 2025