U.S. Municipal Bond Market

The Digital Front Line Runs Through Public Infrastructure, Recent Attacks on Water Infrastructure in at Least Seven U.S. States

Summary

- Federal warnings about critical infrastructure cyber risk are no longer theoretical. For several years now, CISA, NSA, FBI and others have warned that adversaries are targeting the operational technology behind critical and essential infrastructure systems.
- The July cyberattacks appear to be among the most significant publicly reported attacks on U.S. infrastructure so far. The activity began in Minnesota and expanded into a federal warning involving utilities in at least seven states.
- A key issue for public finance where these types of attacks are concerned has to do with **operational resilience**. These attacks test whether public entities can keep essential services operating, communicate clearly, fund recovery, coordinate with partners and shift to manual operations when digital controls are disrupted.

Tom Kozlik
Head of Public Policy and Municipal Strategy
214.859.9439
tom.kozlik@hilltopsecurities.com

Years of Warnings and Two Weeks of Digital Evidence

Federal cyber officials have warned for years that civilian critical infrastructure is no longer separate from geopolitical cyber conflict. In 2023, the Cybersecurity and Infrastructure Security Agency (CISA) warned that cyber actors were targeting programmable logic controllers (PLCs) used in water and wastewater systems. We wrote about attacks related to this warning back in December 2023 in our report titled, U.S. Municipal Water Authorities Targeted With a Different Kind of Cyberattack.

A key issue for public finance where these types of attacks are concerned has to do with operational resilience.

A few months later CISA, the U.S. National Security Agency (NSA) and the FBI warned in February 2024 that Chinese state-sponsored actors were pre-positioning inside U.S. critical public infrastructure for possible disruptive or destructive attacks. The agencies said affected sectors included communications, energy, transportation, and **water and wastewater systems**.

More recent warnings from national security practitioners, cyber experts and from an insurance industry war game help put the late-July 2026 water-system attacks in context as well.

In "Losing the War of the Future," published in the July/August edition of Foreign Affairs, Paul Scharre argued that emerging technologies are changing the economics of conflict by allowing weaker actors to impose outsized costs on stronger actors. Cyber strategies are an example of one of the emerging technologies.

Rob Joyce sharpened the warning in his May 2026 Cyber Defense Review article, "China's Cyber Explosives are in Place. Where's our Response?" He argued that some cyber activity should be understood as preparation for disruption, not routine espionage. The goal, he warned, may be to induce panic and "terrorize our population."

Please see disclosure starting on page 4.

Andy Greenberg's article "What Happens if China Hacks the US Water Supply? I Went to a Secret War Game to Find Out" described a water-system war game for insurance executives and showed how quickly an attack on water utilities could cascade into hospitals, refrigeration, drug manufacturing, and even data centers. One important lesson from the exercise was especially relevant for public finance: according to Joshua Corman, a former CISA strategist, one of the moves participants could have made earlier was to prioritize restoring water in locations with hospitals.

One important lesson from the exercise was especially relevant for public finance: according to Joshua Corman, a former CISA strategist, one of the moves participants could have made earlier was to prioritize restoring water in locations with hospitals.

Taken together, these accounts explain why the recent water-system attacks should be viewed as more than a traditional cybersecurity incident. They show how digital access to local infrastructure can become a tool for physical disruption, public fear and national security pressure. This is not just a threat to public entities and municipal credit. It is a signal that the infrastructure public finance helps construct and the services it supports are increasingly part of the nation's critical security landscape.

Among Most Significant Publicly Reported Attacks, So Far

What began as a cyber incident, seemingly at first isolated to only Minnesota, became a broader warning about the digital vulnerability of U.S. public infrastructure. The danger is not only that public systems are connected. It is that malicious actors can use those connections to disrupt physical services.

The late-July attacks may not yet be the largest cyberattack on U.S. infrastructure, but they appear to be one of the most significant publicly reported attacks on U.S. water and wastewater systems we have seen so far.

What began as a cyber incident, seemingly at first isolated to only Minnesota, became a broader warning about the digital vulnerability of U.S. public infrastructure.

Whether or not this becomes the largest known cyberattack on U.S. infrastructure, it is already an important warning for the public finance community. The attacks targeted the operational technology that connects municipal systems to physical service delivery. That is the important connection cybersecurity experts and federal officials have been warning about. Cyber risk is no longer limited to ransomware, stolen data or back-office disruption. Cyber risk, as expected, is reaching the systems that keep essential public services operating.

What Happened in July?

Minnesota IT Services said more than 30 community water systems were targeted on July 26 and 27, prompting the state to activate its cybersecurity incident response capabilities and coordinate with local utilities, state agencies, CISA, EPA, FBI and other partners. Officials said drinking water remained safe, but several systems experienced operational issues or shifted to manual procedures

On July 30, the FBI and EPA warned that malicious cyber actors, in at least seven states (including Minnesota), had remotely accessed internet-facing operational technology at water and wastewater utilities, changed IP addresses and passwords, and caused a loss of monitoring and control functionality.

Minnesota IT Services said more than 30 community water systems were targeted on July 26 and 27, prompting the state to activate its cybersecurity incident response capabilities and coordinate with local utilities, state agencies, CISA, EPA, FBI and other partners.

CISA separately warned around the same time that threat actors were targeting exposed PLCs in the water sector by changing passwords to lock out operators and changing IP

addresses to disconnect devices. CISA urged water utilities and integrators to remove publicly exposed PLCs and other operational technology from the internet as soon as possible.

CISA urged water utilities and integrators to remove publicly exposed PLCs and other operational technology from the internet as soon as possible.

The cyber activity directed toward water infrastructure moved beyond Minnesota. Michigan publicly confirmed that nine water systems reported activity consistent with the federal warning, while state officials said all systems continued operating safely and there were no known public-health impacts.

Georgia also appears to be in the affected group. Press reports said Georgia water facilities reported similar activity. Other states have not all been publicly identified by federal officials, although reporting has mentioned South Dakota among the locations where related water-system activity was detected or confirmed.

The take-away for public finance related to these attacks is: **this is not only a data-security story, but again it is another operational resilience warning for essential-service infrastructure**.

Not every cyberattack becomes a credit event. Many do not. But the risk to public finance is becoming more direct. When foreign adversaries, proxies, criminals or hacktivists target operational technology, they are not only threatening data. They are testing the systems that keep public services operating. For municipal investors and public officials, the question is no longer only whether an issuer can protect information. It is whether public entities and essential infrastructure can maintain services, preserve public confidence, fund recovery, coordinate with state and federal partners, and operate manually when the digital layer is disrupted.

For municipal investors and public officials, the question is no longer only whether an issuer can protect information.

Recent HilltopSecurities Municipal Commentary

- Inflation and Everything Else, Second Half 2026 Municipal Outlook, July 29, 2026
- The Future of Money, Again: The New Rails of Finance Are Already Being Built, July 22, 2026
- Take-aways from the Hilltop Webinar- In the Era of AI: What is Top of Mind for Two Higher Education Leaders, June 26, 2026
- Oil Relief Ahead of the Fed Could Strengthen Municipal Demand, June 15, 2026
- Hot Inflation, Another Argument for Municipal Discipline, June 10, 2026

Readers may view all of the HilltopSecurities Municipal Commentary here.