U.S. Municipal Bond Market

U.S. Municipal Water Authorities Targeted With a Different Kind of Cyberattack

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

- U.S. Homeland Security's Cybersecurity & Infrastructure Security Agency posted a joint cybersecurity advisory on December 1st referencing cyberattacks on U.S. critical infrastructure or specifically a single-digit number of public water authorities.
- These incidents are not the same as financially motivated ransomware cyberattacks we have seen. These attacks are more similar to those identified in recent Director of National Intelligence and Homeland Security threat assessments.
- The Municipal Water Authority of Aliquippa in Pennsylvania was hacked by CyberAv3ngers an Iranian Government Islamic Revolutionary Guard Corps affiliated Advanced Persistent Threat cyber actor. Other similar attacks have also occurred on other water agencies but this attack in Pennsylvania is the only incident we have details on for now.
- The direct fallout on Aliquippa Water so far has been very minor and we do not expect results from the attack will have an impact on the water authority's credit quality.
- We do not know the details of the other attacks so we are not able to judge the credit impact on those just yet.
- We continue to remain concerned about the potential negative credit impact a cyberattack such as these could have on U.S. state and local governments, critical U.S. infrastructure assets, and other public finance entities.

We continue to remain concerned about the potential negative credit impact a cyberattack such as these could have on U.S. state and local governments, critical U.S. infrastructure assets, and other public finance entities.

Potential for Infrastructure Targeted by Cyber Operations Included in Threat Assessments

Cyberattacks linked to foreign governments directed toward U.S. infrastructure targets should not come as a surprise now. Federal officials have posted and published warnings.

In the third section titled, "Critical Infrastructure Security" of its 2024 Homeland Threat Assessment The U.S. Department of Homeland Security warns of, "physical and cyber threats from domestic and foreign actors—including terrorists, adversarial nation-states, and non-state actors—to the resources, assets, and structures of our critical infrastructure sectors."

In its 2023 Annual Threat Assessment The Office of the Director of National Intelligence not only highlighted the threat cyberattacks pose, but specifically noted, "Iran's opportunistic approach to cyberattacks makes critical infrastructure owners in the United States susceptible to being targeted by Tehran, particularly when Tehran believes that it must demonstrate it can push back against the United States in other domains."

Please see disclosure starting on page 3.

A Joint Cybersecurity Advisory for U.S. Water and Wastewater System Facilities

On Friday Dec. 1, the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) along with other agencies posted a joint cybersecurity advisory titled IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities. CISA explained the advisory is, "to highlight continued malicious cyber activity against operational technology devices by Iranian Government Islamic Revolutionary Guard Corps (IRGC)-affiliated Advanced Persistent Threat (APT) cyber actors."

We saw the foreign government-linked (the IRGC APTs noted above) deployment of cyber assets in the form of a virtual weapon against more than one U.S. critical infrastructure targets.

This advisory is referring to attacks on U.S. critical infrastructure or public water authorities that occurred close to or in November 2023. We saw the foreign government-linked (the IRGC APTs noted above) deployment of cyber assets in the form of a virtual weapon against more than one U.S. critical infrastructure targets. There is only one specific target that has been made public so far.

No Major Credit Impact or Other Fallout So Far from the Cyberattacks, but We See an Increased Threat to Infrastructure Credit Quality Going Forward

This is a reminder that technology is reshaping geo-politics and this advancement is increasing the threat to U.S. infrastructure and municipal credit. The Federal government, "is aware of and examining 'a single-digit'" number of cyberattacks made by a foreign government-linked cyber group (again, the IRGC APTs noted in the CISA advisory) on water sector infrastructure assets in the United States. We are aware of details of one of the attacks that occurred in Pennsylvania.

This is a reminder that technology is reshaping geo-politics and this advancement is increasing the threat to U.S. infrastructure and municipal credit.

On the surface the impact so far from the attack we know about, a cyberattack on The Municipal Water Authority of Aliquippa would probably best be described as very minor, at least for now. CyberAv3ngers, which was labelled as an Iranian Government Islamic Revolutionary Guard Corps affiliated Advanced Persistent Threat cyber actor by CISA, targeted Israeli made water pressure monitoring equipment. That equipment is now running manually. The water utilities' employees noticed the attack rapidly and results from the attack have not impacted water service or quality. The Municipal Water Authority of Aliquippa has a A- "Stable" underlying rating and outlook. As of now we are not expecting results from this attack to have a negative impact on the water authority's credit quality. The Municipal Water Authority of Aliquippa is in Pennsylvania, about 18 miles northwest of Pittsburgh. The water authority serves about 15,000 customers in Aliquippa, and portions of Hopewell, Raccoon and Potter Townships.

There is an important and very distinguishable difference between the attack on The Municipal Water Authority of Aliquippa and the others we do not have details about compared to the cyberattack that occurred recently on The North Texas Municipal Water District.

These attacks on waters systems were not financially motivated ransomware attacks, like those we are used to seeing. These recent CyberAv3ngers cyberattacks are much different. These attacks are close to breaching the civil and military divide compared to cyberattacks we have learned about in the past. These attacks are closer to falling on the range of threats that could include geopolitical actions such as espionage, sabotage or cyber-warfare.

These attacks are closer to falling on the range of threats that could include geopolitical actions such as espionage, sabotage or cyber-warfare.

Like the Director of National Intelligence noted, U.S. critical infrastructure is susceptible to attack, "particularly when Tehran believes that it must demonstrate it can push back against the United States in other domains." This is geopolitical theatre U.S. water infrastructure assets now may increasingly find themselves entrenched within. This is a relatively new, emerging, and increasing risk factor municipal bond market investors need to seriously consider going forward if they are not already.

This is a relatively new, emerging, and increasing risk factor municipal bond market investors need to seriously consider going forward if they are not already.

Monitoring Water Infrastructure Assets

Federal and State law enforcement are investigating the incidents. The Department of Homeland Security's Cybersecurity & Infrastructure Security Agency also published a best practices alert titled Exploitation of Unitronics PLCs used in Water and Wastewater Systems on Tuesday Nov. 28.

On a Dec. 2 social media post CISA reiterated the importance of protecting U.S. water systems. CISA highlighted its Water and Wastewater Systems Sector-Specific Plan published in 2015.

We have been monitoring the landscape for possible cyberattacks on U.S. infrastructure especially since the war in Eastern Europe heated up in February of 2022. We continue to remain concerned about the potential negative credit impact a cyberattack could have on U.S. state and local governments and other U.S. public finance entities. It was also recently reported that hospitals in New Jersey, Oklahoma, New Mexico and Texas were hacked via a ransomware attack before Thanksgiving.

We continue to remain concerned about the potential negative credit impact a cyberattack could have on U.S. state and local governments and other U.S. public finance entities.

Recent HilltopSecurities Municipal Commentary

- Policy Solutions are Taking Shape for Mass Transit, as Expected, Nov. 29, 2023
- President Signs Stopgap Funding Bill, Municipals are a Fitting Option Considering a Wide Range of Economic Outcomes, Nov. 17, 2023
- We Predict $330 Billion of Municipal Bond Issuance for 2024, the Lowest Since 2018, Nov. 8, 2023
- State and Local Credit is Incredibly Resilient, and We Expect Only a Very Limited Credit Impact from Commercial Real Estate Weakness, Nov. 2, 2023

Readers may view all of the HilltopSecurities Municipal Commentary here.