

North Texas water utility serving 2 million hit with cyberattack

By Jonathan Greig

Published: 2023-11-28 · Archived: 2026-04-05 13:46:35 UTC

A water utility serving two million people in North Texas is dealing with a cybersecurity incident that caused operational issues.

With more than 850 employees, North Texas Municipal Water District (NTMWD) provides wholesale water, wastewater and solid waste management services to more than 13 cities in the state, including Plano and Frisco.

Alex Johnson, director of communications for NTMWD, told Recorded Future News that they recently detected a cyberattack affecting their business computer network.

“Most of our business network has been restored. Our core water, wastewater, and solid waste services to our Member Cities and Customers have not been impacted by this incident, and we continue to provide those services as usual,” Johnson said.

“Our phone system was also affected by this incident, and we hope to have it back online this week. NTMWD has engaged third-party forensic specialists who are actively investigating the extent of any unauthorized activity. The investigation is ongoing at this time and includes a review of any potentially impacted District data.”

The incident comes one day after an attack on a Pennsylvania water authority was hit with a cyberattack that reportedly prompted workers to take equipment offline and use backup tools to maintain water pressure.

READ MORE: [Pennsylvania water authority hit with cyberattack allegedly tied to pro-Iran group.](#)

Johnson added that law enforcement was notified of the incident, but did not respond to requests for comment about whether NTMWD is dealing with ransomware.

The cybercrime gang known as Daixin Team said it was [behind the attack](#), adding NTMWD to its list of victims on Monday and claiming to have stolen more than 33,000 files containing customer information.

NTMWD initially [warned](#) customers that its phone lines were down on November 12. That warning is still on the organization’s website.

The ransomware group emerged in June 2022 and [caused significant damage](#) in September 2022 to Oakbend Medical Center, a hospital in Richmond, Texas. The hospital spent weeks recovering after its phone lines and patient record systems were brought down by the attack.

The group also attacked [Fitzgibbon Hospital](#) in Missouri and a German company called [Ista International](#).

Ransomware gangs have targeted water utilities as critical infrastructure organizations likely to pay exorbitant ransoms to restore service.

U.S. law enforcement agencies said ransomware gangs hit [five U.S. water and wastewater treatment facilities](#) from 2019 to 2021 — and those figures did not include three [other](#) widely reported cyberattacks on [water utilities](#).

Richard Caralli, senior cybersecurity advisor at Axio, told Recorded Future News that municipal water is an under-appreciated attack target.

“It has several challenges: limited cybersecurity budget and staff, significant third-party dependencies, and one of the most direct vectors for causing wide-spread effects on life, safety, and health,” he said.

The U.S. Environmental Protection Agency (EPA) sought to [help improve](#) cybersecurity protections at water utilities earlier this year but backed off the effort following [lawsuits](#) from Republican lawmakers and powerful industry groups AWWA and NRWA.

Get more insights with the

Recorded Future

Intelligence Cloud.

[Learn more.](#)

 Recorded Future®

Know what matters.

Act first.

Get started



No previous article

No new articles



[Jonathan Greig](#)

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.

Source: <https://therecord.media/north-texas-water-utility-cyberattack>