



# CYBERSECURITY



**SAINT PAUL REGIONAL  
WATER SERVICES**





### Riviera Beach, Florida Ransomware Attack: City Pays \$600,000

A Riviera Beach, Florida, ransomware attack prompted the city to pay \$600,000 to hackers in a bid to decrypt infected systems.



### BWL paid \$25,000 ransom after cyberattack

Ken Palmer, Lansing State Journal

Published 9:32 p.m. ET Nov. 8, 2016 | Updated 4:26 p.m. ET Nov. 10, 2016



LANING - The Lansing Board of Water & Light paid a \$25,000 ransom to unlock its internal communications systems after a cyberattack last spring.

### Water treatment plant hacked, chemical mix changed for tap supplies

Security

Well, that's just a little scary

By John Leyden 24 Mar 2017

Hackers infiltrated a water treatment plant and changed the mix of chemicals being used.

News Feature | September 6, 2017

## BeaverCountian.com

HOME LOG IN SUBSCRIPTION ABOUT CONTACT

### Iranian-Linked Cyber Army Had Partial Control Of Aliquippa Water System

By John Paul | Nov 25, 2023



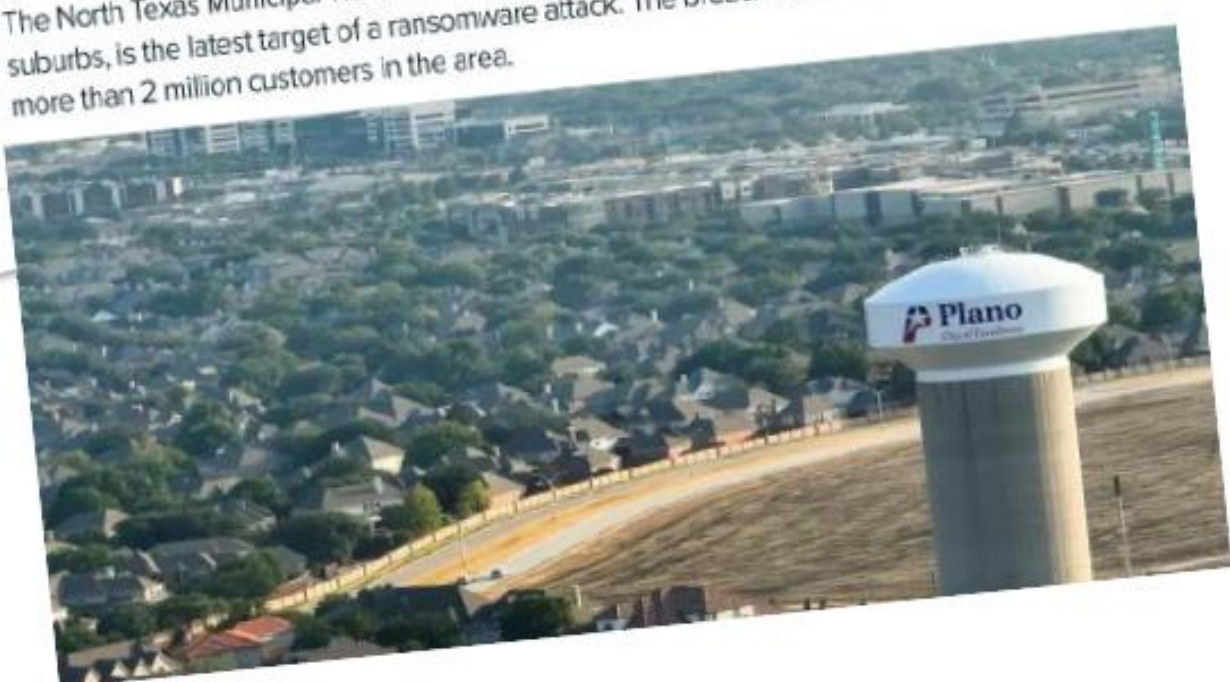
### PRESS RELEASE Kansas Man Charged With Hacking Water Treatment Plant

TOPEKA, KAN. - A Kansas man has been charged with a federal criminal offense of reckless damage to a protected computer system during unauthorized access.



### Investigate Aft Large Texas Water Utility Hit With Ransomware Attack

The North Texas Municipal Water District, which supplies water to sprawling Collin County suburbs, is the latest target of a ransomware attack. The breach has not disrupted service to the more than 2 million customers in the area.





GEOPOLITICS

## Mandiant: Noted breach of Texas

Researchers from the Google recent attacks on critical inf

BY AJ VICENS AND CHRISTIAN VASQUEZ

## Russia-linked targeted Ind



By Sean Lyngaas, CNN

🕒 2 minute read · Published 4

# Inc.

NEWSLETTERS

SECURITY

## FBI Warns on Chinese Cyberattacks as Texas Towns Report Russian Hacks on Water Systems

State-backed attacks on U.S. infrastructure are increasing, and federal law enforcement calls out China's "Volt Typhoon" hacking campaign.

BY SEPTEN

APR 19, 2024



FBI Director Christopher Wray. Photo: Getty Images

g unit linked to

personas are linked to several

claims to have



# DATA DANGERS



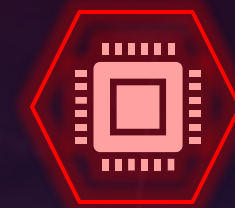
## Data Breaches:

Unauthorized access leading to confidential information exposure.



## Malware Intrusions:

Covert software designed to disrupt computer systems.



## Phishing Attacks:

Deceptive tactics aiming to trick users into revealing sensitive data.



## Denial of Service Attacks:

Overwhelming a system with traffic to disrupt regular functionality.



# CYBERSECURITY POLICY



- Gov Waltz Executive Order – August 30, 2022



- EPA Sanitary Survey Cyber Rule – March 2023

- Legal challenge filed by MO, AR, IA, joined by AWWA, NRWA
- Nationwide injunction July 12, 2023
- Rule withdrawn October 12, 2023



- WH National Security Council Letter to Governors – March 28, 2024

- Requested Governors provide a cyber plan by June 28, 2024



- America's Water Infrastructure Act §2013 round 2 pending

- Enforcement action anticipated



- Cyber Incident Reporting for Critical Infrastructure Rule

- Applies to DW & WW serving >3,300 people
- Comments due July 3, 2024
- Final rule by August 2025



# LEGISLATIVE ACTION



- H.R. 7922, establish a Water Risk and Resilience Organization to develop risk and resilience requirements for the water sector – April 2024

- S. 660/H.R. 1367, Water System Threat Preparedness and Resilience Act – March 2023



# CYBERSECURITY FRAMEWORK (NIST)

- 1 IDENTIFY:** Understand our cybersecurity risks.
- 2 PROTECT:** Implement safeguards to ensure delivery of critical services.
- 3 DETECT:** Develop and implement appropriate activities to identify events.
- 4 RESPOND:** Take action regarding detected incidents.
- 5 RECOVER:** Maintain plans for resilience and restoration of capabilities impaired by incidents.



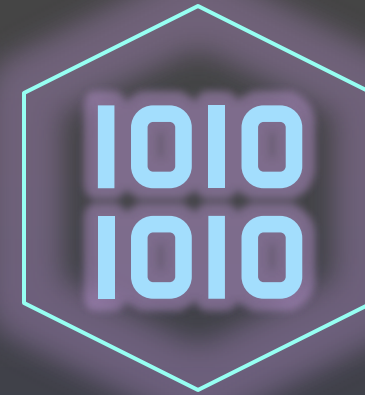


# DATA PROTECTION STRATEGIES



## Access Control:

Managing and restricting access to data to prevent unauthorized usage.



## Data Encryption:

Ensuring secure transmission through robust encryption methods.



## Regular Backups:

Implementing scheduled backups to prevent data loss and aid in recovery.



## Employee Training:

Educating staff on data practices and protocols.



## Incident Response:

Establishing a strategy for addressing data breaches.



# COLLABORATORS/ RESOURCES





# THANK YOU

We are committed to safeguarding our digital infrastructure.

Through continuous monitoring and proactive measures, we prioritize the safety and reliability of our services for the communities we serve.



**SPRWS Cybersecurity Task Force**

