Water, Water, Everywhere
So Why Does No one Seem to Care

Source: **https://www.watereducation.org/aquapedia/wastewater-treatment-process-california**

On July 16, 2022, it was reported that "**The Narragansett Bay Commission, which runs sewer systems in parts of the metropolitan Providence and Blackstone Valley areas, was hit by a ransomware attack on its computer systems.**" The response by the water district was less than forthcoming. In a terse response in an email, "Last week, the Narragansett Bay Commission identified a cybersecurity incident that involved the encryption of data on certain computers and systems in its network."

What you just read is surprisingly pretty much all that has been reported about this incident. Given the history of attacks on municipal water systems over these many years, and the nation's overall heightened awareness concerning the security of critical infrastructure, you'd think there would be a bit more indepth reporting of such an alarming development. In an opinion piece published in **The Hill, May 16, 2022**, Robert F. Powelson, Opinion Contributor, argued that "**the level of cyber sophistication at water systems varies greatly, and because the sector is such a target-rich environment, water utilities are ripe for cybersecurity attacks**."

As in the health care sector, ignoring these threats, and downplaying the impact of systemic attacks, does nothing to harden this critical infrastructure, and offers potential victims a false sense of security.

To bolster his points, Powelson offers two recent examples of attacks on water systems where the attacker exploited a vulnerability in a common remote access application, TeamViewer, that allowed the hackers to have access to old username/password combinations. **As NBC news reported, June 17, 2021**, "On Jan. 15, a hacker tried to poison a water treatment plant that served parts of the San Francisco Bay Area." In this attack, "the hackers were at least briefly

able to order the plant to poison the water" by altering the amount of lye added to the water.

The possibility of attacks coming from Russia on American water systems were top of mind at the beginning of the current conflict in Ukraine. **The EE News reported, February 24, 2022**:

> **The water sector quietly began preparing for a possible onslaught of cyberattacks from Russia more than two months ago, when rumblings of an invasion of Ukraine were being discussed at the White House.**
>
> **Today water utilities across the country are girding for online attacks and misinformation campaigns that could lead to drinking water contamination, service disruptions and demands for ransom.**
>
> **"We don't have any evidence that anything has taken place, or any proof that something will take place," said Michael Arceneaux, chief operating officer of the Association of Metropolitan Water Agencies and the managing director of WaterISAC, the sector's threat sharing organization.**

The fear of compromised water systems is quite real, as indeed it should be, to those charged with defending this nation's infrastructure. As the article cited above states, **"Russia pretty much has the capacity to do what it wants to do, just like [the National Security Agency] has the capacity to do what it wants to do," Arceneaux continued**. "**Whether they do it or not is another question, and which target they pick is another question as well."**

Of course, it is just not the US that finds its water systems under attack. European cybersecurity firm, Stormshield, **published a comprehensive 20 year retrospective of cyber attacks on water systems worldwide.** The first documented attack on a water system, according to Stormshield, happened in the year 2000. This attack was the result of one disgruntled person who did not land the job he wanted with the "Maroochy sewage treatment plant in Australia." As was reported:

> **One of the pumps then stopped working, causing wastewater to be discharged into the seabed, poisoning local flora and fauna, and creating foul odours in the surrounding area... Before succeeding, the individual is thought to have carried out no fewer than 46 attempts to hack the factory's information systems, without ever being detected.**

This attack did, however, prove the "the vulnerability of the world of water to cyber threats."

Water security is a subject I do not think all of our municipal leaders have gotten their minds around. And as is always the case, the smaller the water district is the less resources that water district will have to apply to cyber security.

And those charged with overseeing the effort to keep municipal water systems free of cyberattacks have created an online system to track and monitor cyber events involving water systems. **This new organization called WaterISAC describes itself thusly:**

> **The U.S. water and wastewater sector's leading national associations and research foundations established the Water Information Sharing and Analysis Center (WaterISAC) in 2002, in coordination with the U.S. Environmental Protection Agency. That same year, it was authorized by Congress in the Bioterrorism Act. WaterISAC is the designated information sharing and operations arm of the Water Sector Coordinating Council.**

And what are the best recommendations of this group of wet cybersleuths?

> **Since security is always dependent on multiple layers of protection, it is essential that everyone uses strong and unique passwords, patching is kept up to date, backups are regularly made and stored off the network, and users are given regular awareness training. WaterISAC also advises utilities have cybersecurity incident response plans with constant employee awareness training. Some of its primary recommendations for protecting against cyberattacks include:**
>
> **• Multi-factor authentication;**
>
> **• Anti-virus and anti-malware programs;**
>
> **• Enabling spam filtering to prevent phishing emails from getting through;**
>
> **• Keeping software up-to-date and filtering network traffic that monitors threat indicators; and**
>
> **• Developing and being prepared to implement incident response plans**

Where have we heard all that before? It might has well had come from the advice AOL or Microsoft offer to newbies on the web. Except for the incident response, these are the basics of cybersecurity today. **None of this seems to me to particularly address the newest and most dangerous aspect of securing water systems from cyberattack. The industrial controls themselves that monitor and control these water plants are now under concerted and constant attack.** Defending from these requires a little more effort than running Windows Update, and changing your password frequently, although these are both quite good things to do.

If there was ever a subject that offers up a real world example of the basic tenet of Zero Trust it is water security. The sewage water that runs into the plant gets treated and then sent elsewhere. An error anywhere along the line could have vast consequences far from the actual source of the problem. So Tots and Pears ain't going get the job done.

The river flows
It flows to the sea
Wherever that river goes
That's where I want to be

Flow river flow
Let your waters wash down
Take me from this road
To some other town
— Ballad of Easy Rider, Roger McGuinn (The Byrds)

Back to Top

Gerald Reiff

Back to Top **next post →**