Secret City Tech Whitepaper

American Water: Creating a more resilient infrastructure

Table of Contents

Introduction

The October 2024 cyberattack on American Water, one of the largest water and wastewater utility companies in the U.S., signals yet another wake-up call for critical infrastructure security. Because millions of people rely on this critical service for safe drinking water and sanitation, this attack highlights why it's so important to address cyber vulnerabilities.

The timeline

Let's trace the timeline of the attack, how it likely started, and the best practice architecture that could have mitigated or prevented the American Water cyberattack.

1. Initial Intrusion (October 5, 2024): The attack on American Water was first detected in early October, when cybersecurity monitoring tools flagged suspicious activity within the company's IT systems. Employees reported an unusual system slowdown, and automated alerts indicated possible unauthorized access.

2. Rapid Escalation (October 6-7, 2024): Within 24 hours of detection, the attackers had moved deeper into the company's IT environment. In response, American Water initiated emergency protocols, including isolating key systems to prevent further damage. To contain the breach, critical operational technology (OT) systems — responsible for managing water treatment and distribution — were temporarily shut down.

3. Public Notification and Response (October 8, 2024): American Water notified federal authorities, including the Cybersecurity and Infrastructure Security Agency (CISA), state regulators, and the public. The company reassured customers that water quality had not been compromised, but certain automated operations had been affected, leading to temporary disruptions in water distribution.

4. Ongoing Recovery (October 2024 - Present): As the investigation continued, third-party cybersecurity firms were brought in to assess the extent of the breach and assist in recovery. Manual operations were implemented in areas where automated systems were impacted. While the threat was contained, the company faced a lengthy process of system restoration and reconfiguration.

Impact of the Attack

The impact of the American Water cyberattack appears minimal. A class-action lawsuit was recently filed seeking $5-million in damages on behalf of affected customers, but this is the typical fallout that results from a breach. American Water did not shut down any treatment plants, and although they were forced to temporarily shut down their customer portal, pause billing, and revert to some manual processes, there were no water contamination or public health risks that came out of the attack. Per American Water's FAQ page, it seems business is nearly back to normal.

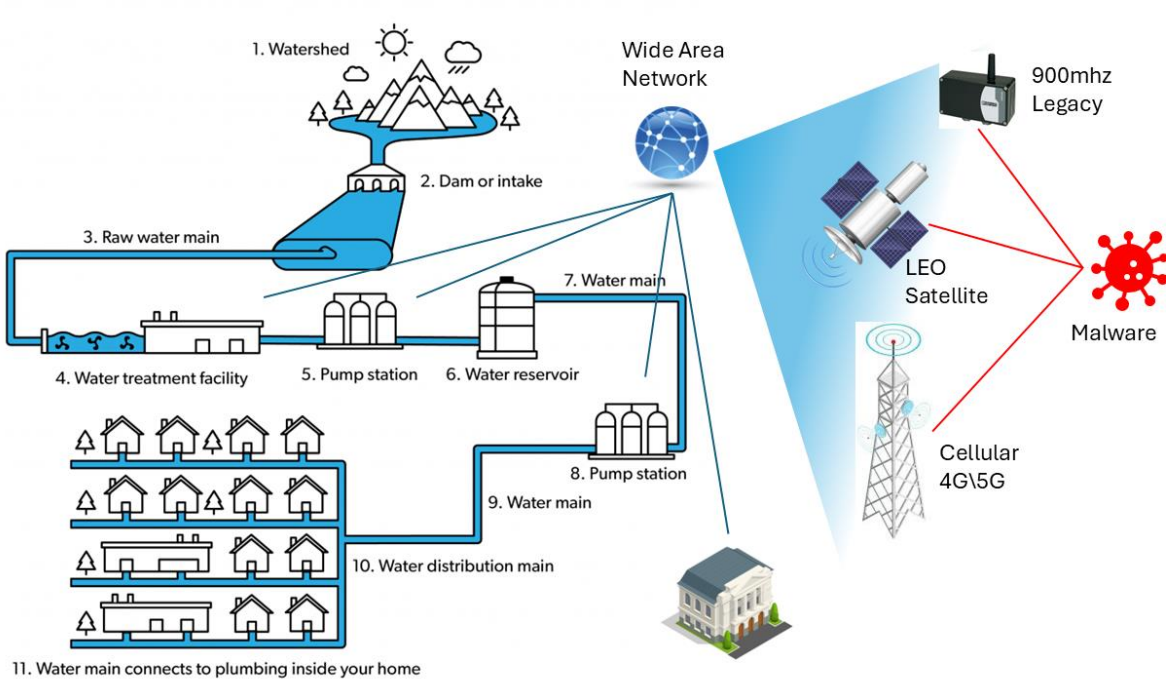
However, the attack could have been worse and shouldn't diminish the need for utilities providers to shore-up their defenses and ensure resilience of their IT architectures. The Oldsmar, Florida incident is an example of how an error or breach can change water treatment chemistry (in this case, adding too much lye to the water supply) and poison a population. There have also been many attempts by U.S. adversaries in which attackers were able to change water chemistry or disrupt automated operations.

Government agencies like the EPA have been warning that attacks on water treatment utilities are increasing. Lawmakers are also calling for inspections of IT systems, such as to ensure best practices are being followed for managing passwords and keeping remote access from Internet exposure and considering civil and criminal penalties for those who don't comply.

How the Attack Likely Happened

The American Water cyberattack is still under investigation. Specifics of how it occurred haven't been released, but several likely scenarios have emerged based on trends in similar attacks:

1. Phishing or Social Engineering: Employees may have unknowingly opened a malicious email attachment or clicked a harmful link, allowing attackers access to the internal network, similar to 2023's Ragnar Locker attacks. Water utilities and other public services often have large workforces, which makes them susceptible to phishing campaigns.



2. Ransomware: There are indications that ransomware may have encrypted key files and systems. This problem is similar to what happened during the MGM hack. Ransomware attacks on critical infrastructure have increased in recent years, with attackers locking companies out of their own data and demanding payment to restore access.

3. IT/OT Integration Vulnerabilities: Water utilities often rely on a hybrid network where both information technology (IT) systems and operational technology (OT) systems are integrated to monitor and control water purification, distribution, and wastewater management. While this setup improves efficiency, it can also create additional vulnerabilities if the two environments are not properly segregated. Once attackers gain access to the IT network, they can use it as a bridge to reach OT systems, which are typically less secure.

4. Internet-Facing Systems: In the past, the Chinese-sponsored hacker group Volt Typhoon took advantage of firewalls that were connected both to the internet and to critical control systems. This approach also takes advantage of a lack of control plane segregation, as hackers can remote-in via internet-facing systems and gain management access to critical systems.

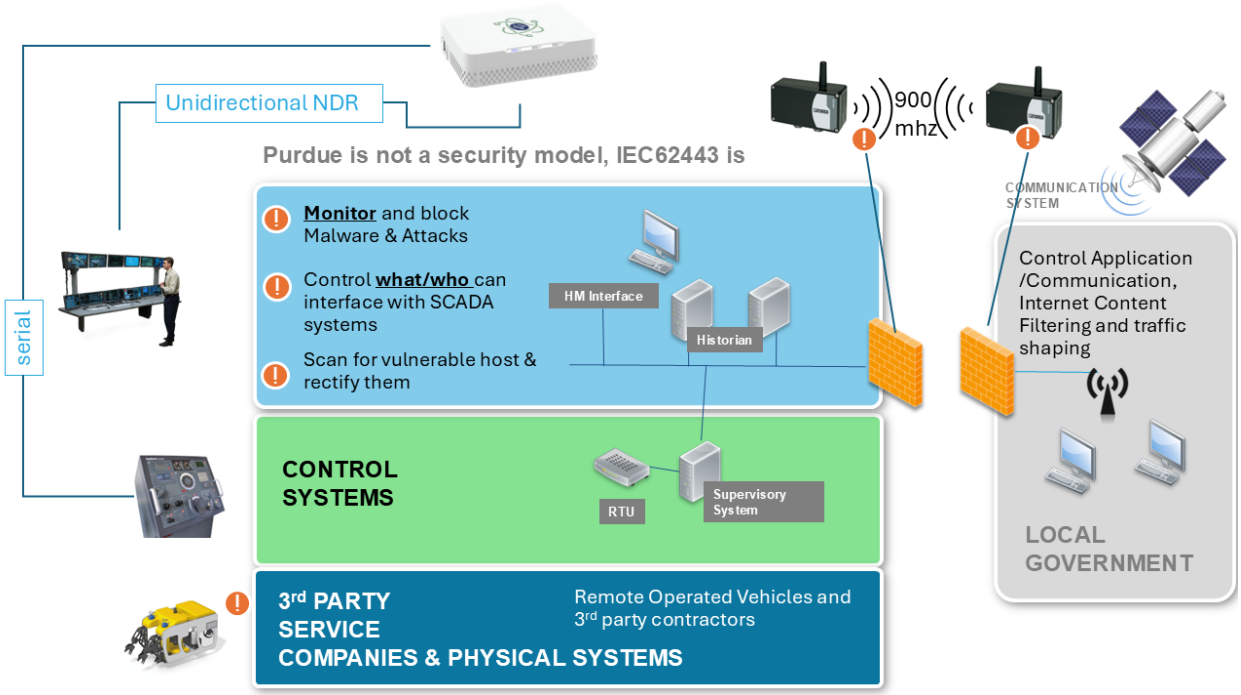
The Solution: Cyber-Physical Rescue)

Very similar to the global CrowdStrike outage, the most important takeaway from the American Water cyberattack is that organizations need the ability to recover fast. Remote access solutions help with this, but it matters how these solutions are architected and which capabilities they offer.

The traditional approach is to gain remote access via a direct link to the affected systems. The problem with this is that when these systems are breached, encrypted, or offline, it's impossible to remote-into them. This requires teams to physically connect to and revive systems (as with the CrowdStrike incident), or worse – completely replace their infrastructure, as Merck did during the 2017 NotPetya breach.

Image: Traditional remote access relies on a direct link to production equipment or in-band ethernet for detection systems. Log management remains an issue over wireless WAN technologies

Cyber-Physical Response combines many older technologies such as serial and simple log management to detect and protect critical systems in a very different and scalable way. SCT creates a management network or out of band serial connection that is completely independent of production network equipment, an architecture that resembles out-of-band (OOB) management, but it allows for grabbing back control of the system at a distance if disaster strikes. This gives teams a lifeline to their main IT and OT systems, including servers, switches, sensors, controllers, and other critical assets, even when their main systems are offline.



Here's how CPR and out-of-band management could have helped mitigate the effects of the American Water attack:

1. Enhanced Containment: By isolating the network used for system control and monitoring, OOB management could have ensured that even if the primary network was compromised, attackers would not have been able to access or disable key operational systems. This would have limited the need to shut down OT systems and prevented widespread operational disruption.

2. Faster Recovery: With isolated management infrastructure, administrators would have been able to access critical systems remotely, even during the attack. This capability enables faster diagnosis of the issue and restoration of services without relying on compromised networks. In the case of a ransomware attack, for example, OOB management can help initiate recovery operations from backups, minimizing downtime.

3. Reduced Attack Surface: By creating an independent network with fewer access points and stricter controls, OOB infrastructure reduces the chances of attackers exploiting vulnerabilities. This removes critical systems from directly facing the internet and significantly reduces the attack surface. It's an additional layer of security that complicates attempts to breach sensitive control systems.

What if organizations already have a incident response or cybersecurity solution?
Having a completely independent management architecture is the foundation of CPR. But, an equally important facet is what kind of capabilities do teams have when they use CPR. Traditional out-of-band solutions allow basic remote console access and some automation. These are great for troubleshooting or applying regular updates, but during a major attack or outage, systems often must be completely destroyed and rebuilt/reimaged.

This is where CPR comes into play. These systems with their services combine the full stack of management capabilities (routing, switching, jumpbox, cellular, etc.), but also handles logs and early indications of attacks and checks against the assets or machinery (attack surface) that are under attack. This enables teams to not only gain reliable access via multiple WAN links, but also to completely rebuild affected infrastructure remotely.

Find out more about CPR

The American Water cyberattack is another wake-up call for critical infrastructure providers to rethink their cybersecurity strategies. Isolated Management Infrastructure is the key approach to retaining control during an attack but requires the robust capabilities of Cyber-Physical Rescue ensures rapid recovery to help utilities and essential services fortify their infrastructure, Engage with Secret City Tech now to find out the best practices architecture and become resilient against cyberattacks.

About the Author

James Cabe….

Secret City Tech

Based near Oak Ridge, TN, we specialize in securing Operational Technology (OT) environments. As cyber threats evolve, OT security is no longer a DIY task. Industrial control systems face unique challenges that require specialized expertise. We provide robust cybersecurity solutions tailored to the needs of critical industries.