Water Companies Must Rethink Cybersecurity Strategy to Prepare for the Next Big Cyber Attack

In October 2024, **American Water Works Company Inc.**, the largest publicly traded water and wastewater utility in the U.S., disclosed a significant cybersecurity breach. The company, which serves over 14 million customers across 14 states, had to disconnect several key systems, including its customer billing portal, in response to unauthorized activity within its IT infrastructure. Though water and wastewater operations were reportedly unaffected, the breach highlights a growing concern: **water utilities are increasingly being targeted by cybercriminals**.

The Scale of the Problem

Water infrastructure is a prime target for cybercriminals and nation-state actors alike. Attacks against water utilities are increasing, and experts warn that water systems are among the most vulnerable of all critical infrastructure sectors. As reported by **CNN**, the attack on American Water follows several high-profile breaches of U.S. infrastructure, many of which have been linked to geopolitical rivals, including **Russia, China, and Iran**.

According to a **report by TechTarget**, American Water's quick response involved disconnecting systems and enlisting the help of third-party cybersecurity experts, demonstrating the company's preparedness. But the fact that such a breach could occur in one of the largest, most resource-equipped water utilities indicates how vulnerable the sector remains.

Water utilities represent a crucial element of public safety and disrupting them can have severe consequences for public health, economic stability, and even national security. In recent years, cybercriminals have attempted to access operational technology in water treatment plants, such as when hackers compromised a water filtration system in a small Texas town earlier this year. In that instance, the attackers attempted to alter the chemical levels in the water supply—a chilling reminder of the potential for physical harm.

The **FBI** has warned of cyber espionage efforts targeting water treatment facilities, electrical grids, and transportation systems as part of broader campaigns aimed at destabilizing U.S. critical infrastructure. Water utilities, as essential providers of drinking water and wastewater management, are at the center of this storm.

Vulnerabilities and Regulatory Concerns

One of the most alarming factors contributing to these attacks is the lack of basic cybersecurity measures in many water systems. The Environmental Protection Agency recently conducted an assessment that revealed 70% of the water systems inspected do not comply with the cybersecurity requirements outlined in the Safe Drinking Water Act. Common issues included outdated software,

default passwords that had never been changed, and systems that still allowed access to former employees.

In its recent enforcement alert, the EPA described these vulnerabilities as "alarming," given the critical nature of the services water companies provide. Water systems are essential to public health and safety, making them prime targets for cybercriminals and hostile nation-states. In many cases, these attacks have the potential to cause widespread service disruptions, contamination of water supplies, or even complete shutdowns of water treatment facilities.

As seen in the **TechTarget** report on American Water's breach, public utility companies are increasingly targets because of the disruption potential. While American Water's operational systems were reportedly unaffected, the breach disrupted customer-facing services, such as billing, and raised concerns about data exposure. The increasing frequency of these incidents demonstrates that cybercriminals view water utilities as high-value targets, knowing that even a partial disruption can have widespread consequences for both consumers and businesses.

Why Water Companies Need a New Cybersecurity Approach

The days of water companies being immune to major cyber incidents are over. Hackers are now aggressively targeting critical infrastructure, and water systems are high on their list. To prepare for the next big cyberattack, water companies must adopt a proactive cybersecurity strategy that includes:

1. **Comprehensive Risk Assessments**: Companies need to assess their entire network, from operational technology to information technology, to identify and address security gaps. This includes updating software, replacing legacy systems, and eliminating default passwords or single login setups.
2. **Regular Audits and Compliance Checks**: With many water systems failing to meet even basic cybersecurity standards, it's crucial to conduct regular audits and compliance checks. Water utilities should align with frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the EPA's cybersecurity guidelines to ensure they are meeting regulatory standards and mitigating risks.
3. **Improved Network Segmentation**: Segregating critical operational systems from less secure customer-facing systems is essential. This helps to prevent cybercriminals from gaining access to water treatment operations through vulnerable entry points like customer service portals, as seen in the American Water incident.
4. **Incident Response Planning**: Water companies must have a robust incident response plan that is regularly updated and tested through tabletop exercises. This includes training staff on how to detect and respond to cyber threats quickly, minimizing downtime and damage during an attack.
5. **Collaboration with Government and Industry Experts**: Partnerships between water utilities, government agencies, and cybersecurity experts are vital. These collaborations can provide early threat intelligence, cybersecurity guidance, and the resources needed to recover quickly after an incident.

6. **Proactive Threat Hunting and Monitoring**: Real-time monitoring and threat hunting are essential to detect cyber threats before they escalate into full-scale attacks. Companies must invest in next-generation detection and response tools to stay ahead of attackers.
7. **Security Awareness Training**: Employees are often the weakest link in cybersecurity, and water companies are no exception. Regular security awareness training can help staff recognize phishing emails, suspicious activity, and other common attack vectors.

Preparing for the Next Big Attack

The recent attack on American Water is not an isolated event but rather part of a larger wave of attacks targeting critical infrastructure across the U.S. It is only a matter of time before another water utility is targeted, and the consequences could be far more severe. Water companies must rethink their cybersecurity strategies now, before they find themselves in the crosshairs of the next major attack.

Cybercriminals and nation-state actors have demonstrated their ability to compromise water systems with ease. Without significant investments in cybersecurity, water utilities will remain at high risk of service disruptions, data breaches, and public health crises. The time to act is now, and water companies must prioritize cybersecurity to protect their critical services and the communities that depend on them.

In the words of cybersecurity expert Adam Isles, "Water is among the least mature in terms of security." As threats continue to escalate, water utilities must mature their cybersecurity postures, or they risk becoming the next victim of a devastating attack.

Who is Waintraub Cyber Solutions?

Waintraub Cyber Solutions was incorporated in 2020 with the small to medium sized business in mind. At WCS, we understand that every organization's cybersecurity needs are unique. Our goal is to provide top-tier cybersecurity services tailored to protect your business from evolving digital threats while ensuring rapid incident response when it matters most. Whether you require immediate containment, proactive monitoring, threat assessments, or long-term digital resilience, our experienced team is ready to serve.

References:

CNBC: Biden admin, U.S. ports prep for cyberattacks as nationwide infrastructure is targeted
CNN: American Water, largest U.S. water utility, targeted by cyberattack
TechTarget: American Water discloses breach, utilities unaffected
Mandiant Report: State-linked Cyber Attacks on U.S. Water Infrastructure
CISA: Incident Response Guide for Water Utilities