THREATLOCKER

Protecting Water Infrastructure Against Cyberattacks

Like many critical infrastructure verticals, the water industry faces increased cybersecurity risks.

Water is managed locally or privately depending where you live, making it incredibly difficult to regulate and manage. As far as utilities go, water typically has the lowest amount of financial resources allocated towards it, making cybersecurity a non-priority. On top of that, OT has been retrofitted for remote access creating an inherent cybersecurity issue.

As threat actors look to disrupt supply chains, water companies need to ensure water's continued access and safety. As with all verticals, water companies need to be concerned about the regular threats that all businesses face. As the risk of ransomware and other cyber attacks continues to increase, water companies must be vigilant of attacks targeting their infrastructure.

Typically, when a business loses access to its system due to a ransomware attack, it does not affect people's ability to survive. Problematically, decentralized regulatory control and limited finances often mean that companies lack the resources for continuous hygiene. Meanwhile, cyber-physical (CPS) technologies link enterprise IT networks to operational technology (OT) networks increase the chances that a threat actor's attack will be successful.

Organizational Status

Across the industry, companies are managed differently. According to the Water Sector Coordinating Council's "Cybersecurity 2021 State of the Industry":[1]

- 51.4% of survey respondents are with a department of a municipality or county.
- 32.7% of survey respondents are with a special district or independent government entity.
- 9.3% of survey respondents are with a private non-profit/cooperative.
- 6.4% of survey respondents are with a privately-owned or investor-owned utility.

With water companies owned and operated in various ways, the financial support for cybersecurity varies widely.

Cyber Risk and Visibility

While threat actors continue to target critical infrastructure, few statistics exist when compared with enterprise IT. An article from 2021 "A Systematic Review of the State of Cyber-Security in Water Systems" explains that the attacks are rarely made public and that attribution is often difficult.[2]

However, the article does note that the number of attacks on cyber-physical (CPS) systems has increased in recent years, listing attacks like Stuxnet, DuQu, BlackEnergy, and Havex. Moreover, the report additionally notes that threat actors targeting water systems include nation-state political actors, cybercriminal financial actors, and former employees.

---

[1] American Water Works Association. (2019). Water Sector Cybersecurity Risk Management Guidance. American Water Works Association. https://www.awwa.org/Portals/0/AWWA/ETS/Resources/AWWACybersecurityGuidance2019.pdf?ver=2019-09-09-111949-960

[2] Tuptuk, N.; Hazell, P.;Watson, J.; Hailes, S. A SystematicReview of the State of Cyber-Security in Water Systems.Water2021,13, 81. https://dx.doi.org/10.3390/w13010081

Anatomy of a Cyber Attack

The traditional method for protecting OT systems from IT and vice-versa is air-gapping, an interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control). OT systems often run legacy operating systems, and not only pose an increased risk of being exploited themselves as a result of a vulnerability, but also allow attackers to access IT systems by running undetected code on the OT systems. However, water companies increasingly use CPS technologies that connect their OT systems to the enterprise IT network. This allows for more efficient monitoring and integration into billing services.

How the Attack Works

This connectivity undermines air gapping because threat actors can use a vulnerability in the enterprise IT network to gain access to OT. Attackers often start by using a common vulnerability, malicious software or Remote Access Tools (RATs) to access the enterprise network. Once they gain access, they escalate the attack by either using direct controls over OT systems, or exploit poor code in the CBS.

They will often exploit privileges within that network, or operate silently from the OT operating systems allowing them to capture information on the IT networks. From there, administrative privileges are obtained to operate in the IT network with admin permissions.

For example, when threat actors attacked a water treatment plant in Oldsmar, Florida this year, they started by exploiting TeamViewer, a legitimate piece of software, in order to access the IT systems. This ultimately gave them access to the OT systems, enabling them to increase the sodium hydroxide levels to potentially dangerous amounts. In this case, the attacker went in for the kill and attempted to potentially poison the water systems. However, in many cases there would be backdoors planted which could allow further access.

Why The Attack Is Successful

Many OT systems were built and designed prior to the internet, meaning that they incorporate legacy technologies. Between design and age, they lack modern security controls, and security tools like scanners are often unable to provide adequate visibility into assets on the network.

These systems are often fragile. A small change or abnormal activity within the network architecture can lead to costly downtime. For the water industry, downtime has greater social implications. Water is fundamental to health and hygiene. Therefore, critical system outages can impact the population's physical safety.

Municipalities are notorious for having bad IT hygiene. Users often run as local administrators with outdated operating systems and poor training, and fail to implement basic controls listed in CIS and NIST frameworks.This makes them attractive targets for cybercriminals which leads to major societal implications.

Cybersecurity Budget Allocation

Despite the rise in attacks against CPS technologies, water companies continue to struggle with limited IT and OT financial resources.

The "Cybersecurity 2021 State of the Industry" notes the following around IT and OT cybersecurity budget allocation:

- 38% of systems allocate less than 1% of budget to IT cybersecurity.
- 22.1% of systems allocate 1–5% of budget to IT cybersecurity.
- 6.3% of systems allocate 6-10% of budget to IT cybersecurity.
- 4.1% of systems allocate greater than 10% of budget to IT cybersecurity.
- 44.8% of systems allocate less than 1% of budget to OT cybersecurity.
- 20.95% of systems allocate 1–5% of budget to OT cybersecurity.
- 4.9% of systems allocate 6-10% of budget to OT cybersecurity.
- 1.7% of systems allocate greater than 10% of budget to OT cybersecurity.

These limited budgets ultimately make securing water more difficult, driving companies to seek cost-effective cybersecurity risk mitigation solutions.

Decentralized Regulatory Requirements

To further complicate matters, water companies lack clear regulatory guidelines. Despite falling under the Environmental Protection Agency's (EPA's) control, water companies also find themselves regulated by state and environmental agencies as well as state public utility commissions.

Although the America's Water Infrastructure Act of 2018[3] included cybersecurity, it only mentions it twice, providing limited guidance:

> The emergency response plan shall include— '(1) strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system;

The EPA provides a four-page "Water Sector Cybersecurity Brief for States"[4] which lists the 2019 Water Sector Cybersecurity Risk Management Guidance (WSCRMG).[5]

As water companies look to protect themselves from ransomware attacks, some controls listed in the WSCRMG that enable them include:

- Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.
- Access control for the management, monitoring, review, and audit of accounts established including access control, account roles, privilege accounts, password policies and executive oversight.
- Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies.
- Workstation and other equipment authentication framework established to secure sensitive access from certain high-risk locations.
- Privileged programs controls established to restrict usage of utility programs that could reset passwords or override controls as well as enterprise system audit tools that can modify or delete audit data.

---

[3] America's Water Infrastructure Act of 2018, https://www.congress.gov/115/bills/s3021/BILLS-115s3021enr.pdf

[4] Environmental Protection Agency. (n.d.). Water Sector Cybersecurity Brief for States. EPA. https://www.epa.gov/sites/production/files/2018-06/documents/cybersecurity_guide_for_states_final_0.pdf

[5] American Water Works Association. (2019). Water Sector Cybersecurity Risk Management Guidance. American Water Works Association. https://www.awwa.org/Portals/0/AWWA/ETS/Resources/AWWACybersecurityGuidance2019.pdf?ver=2019-09-09-111949-960

- Policies and procedures established for network segmentation including implementation of DMZs based on type and sensitivity of equipment, user roles, and types of systems established.
- Program for hardening servers, workstations, routers, and other systems using levels of hardening based on criticality established. Program should include policies and procedures for whitelisting (deny-all, allow by exception).
- Remote access framework including policies and procedures established to provide secure access to telecommuting staff, established for the management, monitoring, review, and audit of remote access to the organization.

How Locking Down Application-to-Network and Application-to-Application Communication Enhances Security

With ransomware on the rise, water companies need to find threat mitigation strategies that enable them to protect their OT environments. The same connectivity that enables threat actors to move from enterprise IT networks to OT systems also acts as a means of transmitting malware to OT devices.

Installing security updates to endpoint IT devices is fundamental to protecting interconnected systems. However, even a single unpatched endpoint can pose a risk to OT systems. Additionally, because OT systems are fragile, updating the endpoints creates an additional risk. This added complexity often requires the water company to schedule maintenance and downtime. Again, since water is fundamental to human health and safety, this is not always a viable option.

By setting deny-all policies for all application communications to networks and other applications, organizations limit access as much as possible. Some benefits of this approach include:

- Blocking device and application access to prevent malware from executing on a device.
- Limiting what applications can access the internet to minimize the risk of threat actors exploiting a software vulnerability.

- Limiting what applications can be used at the same time to minimize the risk that malware can be transferred to applications that require privileged access.
- Limiting data sharing between applications to minimize the risk that malware can be transferred from one application to another.
- Limiting devices and applications to resources to minimize the risks that information can be posted or processed on publicly accessible information systems.
- Ensuring the principle of least functionality to minimize risks associated with what applications can run in an environment, what applications can connect to the internet, and what devices can be used to access resources.

ThreatLocker® is a global cybersecurity leader, providing enterprise-level cybersecurity tools to improve the security of servers and endpoints. ThreatLocker's combined Application Whitelisting, Ringfencing™, Storage Control and Privileged Access Management solutions are leading the cybersecurity market towards a more secure approach of blocking unknown application vulnerabilities.

To learn more about ThreatLocker visit: www.threatlocker.com