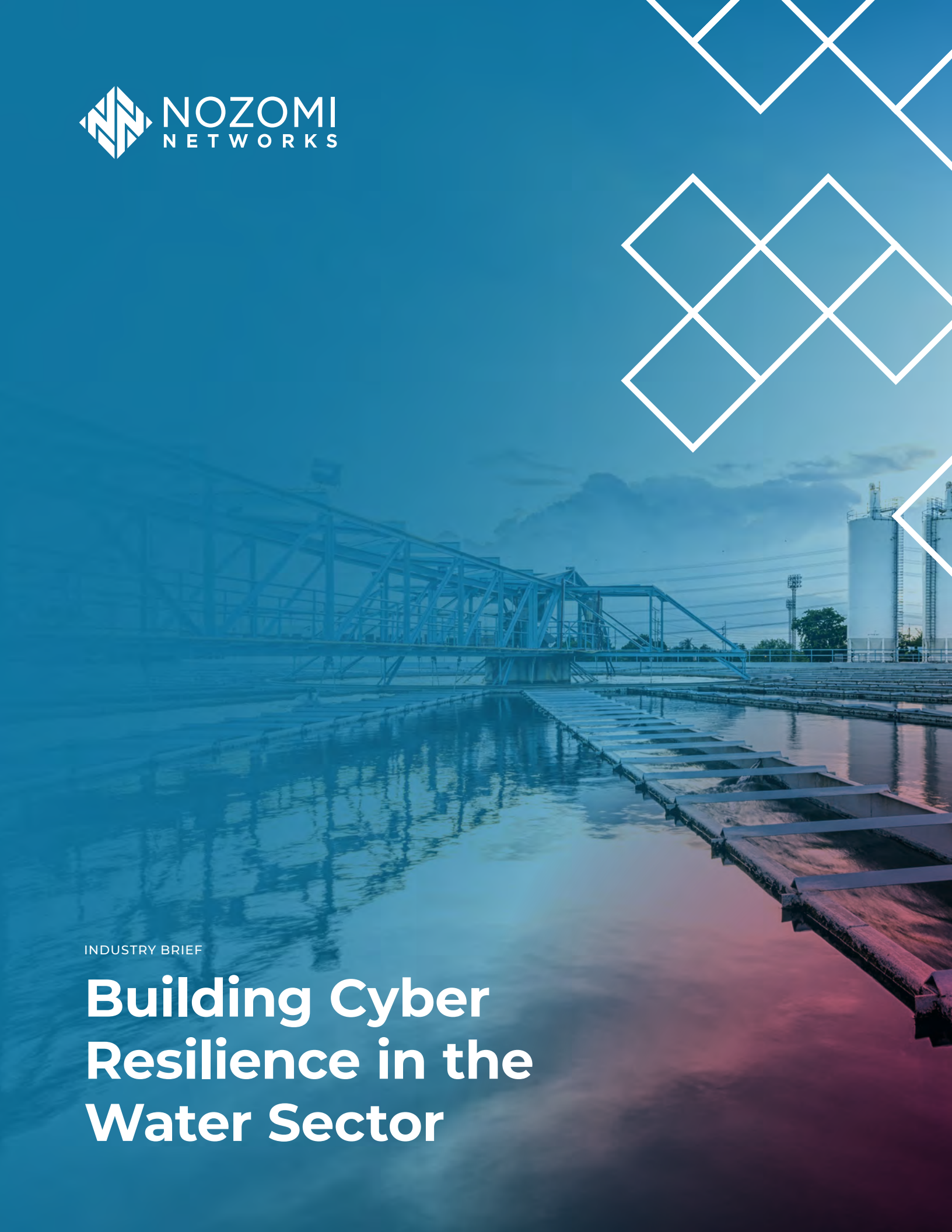
NOZOMI NETWORKS



INDUSTRY BRIEF

Building Cyber Resilience in the Water Sector

Table of Contents

1. Introduction

Cyber Resilience in the Water Sector

Water utilities provide a critical service to the community and host a large amount of valuable data, making them vulnerable to attack. In the years ahead, as threats continue to evolve, critical infrastructure will likely become an even more popular target. This industry brief explains the growing cyber threats that water utilities worldwide are facing in increasingly automated and digital environments, as well as how organizations can prevent or minimize damage from attacks.

Historically, water utilities have not considered themselves to be at great risk of attack. This is because they have traditionally been manually operated and not connected to any online networks. However, like most industries, water utilities have undergone a digital transformation and are more connected than ever, with automated processes and Industrial Internet of Things (IIoT) both a core part of modern set-ups.

Unfortunately, security mindsets have not kept pace with this transformation. A survey from the Water Sector Coordinating Council estimates that 38% of water utilities in the United States only allocate 1% of their budget to cybersecurity, a product of both limited finances and an underestimation of risks this industry faces.[1] This has delayed important investments in cybersecurity and resulted in a sector that is not strategically prepared for the more serious attacks that are occurring. Non-state actors have accelerated the severity and regularity of attacks launched against water utilities, with Iranian and Syrian groups hitting facilities in recent years.

It is important that our water utilities' cyber-defense capabilities adapt to these threats, and that decision-making and planning takes a long-term and holistic approach. Unfortunately, the water sector needs to change and adapt to meet the threats of the future. A securely defended water sector can be achieved by enhancing existing practices, authorities, and budgets to build resilience. Institutions also need to build new and unique programs and create funding structures to bolster the work and oversight of the EPA and sharpen the focus on rural infrastructure. Utilities must develop innovative plans that help them anticipate, diagnose and respond to threats and to protect water assets.

There are a variety of types of actors targeting water utilities. These include internal and external threats, ranging from employees to malicious state-sponsored groups, each with a variety of ways to target and launch attacks. While ransomware is the most commonly referenced attack style, malware in critical infrastructure can manipulate control systems used to operate equipment and machinery and infiltrate networks in order to access private data.

The sector as a whole is facing unprecedented challenges with similar risks and similar vulnerabilities. There is no 'one-size-fits-all' approach to security, but there are proven ways to face the greatest gaps and weaknesses.

> **38%** of U.S. water utilities allocate only **1% of their budget to cybersecurity** due to both limited finances and an underestimation of cybersecurity risks.
>
> *Source: Water Sector Coordinating Council*

2. Cybersecurity Challenges for the Water Sector

Globally, the water and wastewater sector is worth nearly $500 billion USD.[2] Water is an incredibly important resource not only for human life, but also for sectors that depend on access to water to operate and sustain economic growth. As an example, the agriculture sector accounts for 70% of global water usage and is estimated to employ 50-90% of the world's population.[3] Despite its significance as a critical sector, only 23% of utilities surveyed stated they perform annual cybersecurity risk assessments according to a report by Water Information Sharing and Analysis Center (Water-ISAC) in the U.S..[4]

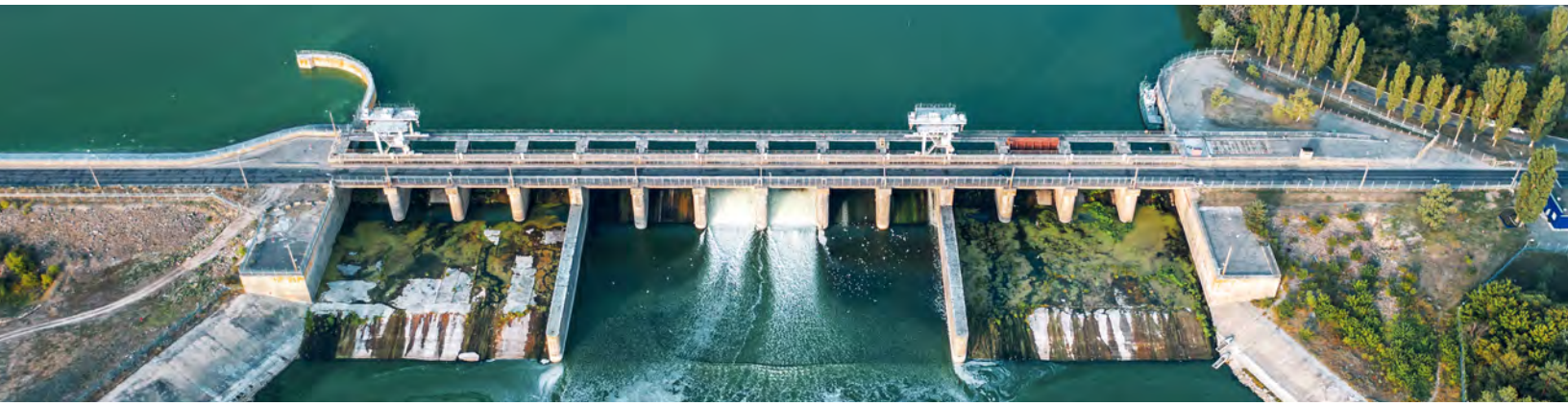
The water sector is in a period of significant transformation, leading to more opportunities for prosperity and development. The rapid adoption of remote systems, increased automation, and wider connectivity is changing the way services are delivered and improving access to clean water for millions of people.

Due to its unique structure, investment in cybersecurity has lagged in the water sector. Water utilities have traditionally existed in silos, with each utility operating independently and with most operations occurring on site. This autonomous design has limited resource sharing, and utilities are often unaware of the threats facing the broader industry.

Ownership is a mix of public and private; some utilities service a huge area while others only a few thousand people. The decentralized and autonomous nature of the water sector means there is little standardization across engineering practices or ownership. The disparate nature of these facilities has hindered efforts to create a standardized approach to security and has made it difficult to gauge the unique risks the sector faces.

Water supply and wastewater disposal utilities have rapidly adopted information technology (IT), operational technology (OT) systems, and industrial internet of things (IIoT) technologies. ICS and OT networks are generally considered to be highly vulnerable to cyberattacks and difficult to secure.

> “
>
> Despite its significance as a critical sector, only **23% of utilities** surveyed stated they **perform annual cybersecurity risk assessments**.
>
> *Source: Water Information Sharing and Analysis Center (Water-ISAC)*



2.1 Cyber Threats to Water Utilities

Cyberattacks against water utilities have the potential to cause financial loss and disruption to critical services. It is important that these utilities have full transparency over their digital footprint and have mechanisms in place to adapt to the changing threat landscape. Cyberattacks are increasing in frequency and complexity, and the water sector needs to keep pace with the growing threat environment.

Attacks have become more sophisticated since a 2002 Australian attack which utilized radio signal to disrupt a sewerage system, but these vulnerabilities remain. The supervisory control and data acquisition (SCADA) system used in this attack is still in use in water facilities across the world. Digitization continues to transform the way these services are deployed and allows utilities to better react to the changing needs of business and citizens. Networked industrial control systems (ICS) used to manage physical processes are now standard in water utilities, and remote access is commonly used to manage multiple systems. Increased automation and connectivity have brought positive developments in the way data is shared and stored, making processes more efficient and effective.

Threats to water utilities range from internal—negligent human error, intentional, or insider knowledge from former employees—to external, including terrorism and organized crime, and malicious nation-state or state-sponsored actors. As a result of a cyber incident, data may be lost, equipment malfunctions may half operations, and water quality can be compromised. Water plants may also open themselves to legal action relating to data breaches, including large insurance claims, personal injury, and damage claims. Water utilities' irreplaceable role in our lives and industries considerably enhances their value as a target that tolerates little downtime. For malicious actors, hostile states, or organized crime syndicates, this makes water a lucrative target.

Attacks on critical infrastructure such as water have the capacity to create physical harm and produce fear and panic across communities. Major technological advancements in recent years have revolutionized how water facilities and systems operate; however, for many organizations, cybersecurity protections have not kept up. Governments globally rely on industry collaboration to protect critical assets, especially for water which typically straddles the quasi-government-private space.

2.2 Challenges in Responding to Cyber Threats

Public and private sector have been slow and siloed when it comes to defending against cyber threats. The sector is behind in terms of deep analysis and understanding of the threat landscape, and investments in cybersecurity thus far. Water security impacts more than just households: within hours of an incident, effects can be felt across government, health, transportation, and food sectors.

Utilities are often decentralized and autonomous, operating as a sole unit within a district and not directly connected to a greater system. Smaller utilities may not have the same number of resources to divert to cybersecurity, and the larger utilities may struggle to secure the large spread of communications and automation resources.

Resource constraints prevent utilities from updating solutions, improving internal processes, identifying spare budget, and procuring new security services. Having access to the right skills, people, and systems closes some of the gaps for cyberthreats to access.

There is no single overseer or set of security standards in the water sector. The Environmental Protection Agency (EPA) has some jurisdiction, as does the American Water Works Association (AWWA), and the Water Information Sharing and Analysis Center (WaterISAC). Standards and increased security requirements are currently under consideration by government and non-governmental bodies, however, more needs to be done to build a collaborative response to water security threats.

2.3 Timeline of Attacks on Water Facilities

Since 2000, there have been multiple attacks on water facilities ranging in severity, which caused disruption to services and cost millions of dollars in response and remediation.

2000

Queensland, Australia

A disgruntled former employee hacked the water sewage plants in Queensland, Australia, letting out **over a million liters** of sewage over a period of several months.

2013

New York, U.S.

Iranian hackers infiltrated a dam in New York, **costing $30,000 to repair**.

2016

Michigan, U.S.

A phishing operation locked the Lansig Board of Water and Light out of their systems. Lansig paid **$25,000** to recover access and **$10 million** to replace affected computers and software.

2017

U.S.

A Syrian group was able to alter the **chemical dosing** at a U.S. water utility.

2018

Georgia, U.S.

The City of Atlanta suffered a ransomware attack which disrupted city utilities and prevented to Department of Watershed Management from accessing their work computers for nearly a week. **Recovery costs were up to $5 million.**

2020

South Carolina, U.S.

Greenville Water in the U.S. had their online payments system compromised, affecting **500,000 residents.**.

3. Threat Summary

Threats to water facilities can be categorized as either internal or external. Internal threats include negligent, compromised, or malicious humans contributing to system faults or impacting the systems. External threats include targeted malicious actions, from terrorism or organized crime all the way up to state-actors in a conflict setting.

3.1 Internal Threats

According to IBM, human error is the leading cause of cybersecurity breaches, accounting for 95% of cases. Sources of human error include current and former employees, employees lending devices to family members, and clicking on phishing links. Insider knowledge of how these systems operate can also be damaging to a facility. Former employees who retain this knowledge pose a significant risk. A global 2016 Survey from PWC found that 28% of CEOs and C-suite executives believe that insiders were a contributing factor to breaches, which includes former employees and external contractors.[5]

Other sources of human error include weak passwords, incorrectly configured networks or devices, or office social elements such as sharing passwords and leaving computers unattended. Many employees undertake cybersecurity training as part of an onboarding process, however the significance of some of the risks may not always be clearly stated. Training also needs to be consistent—cyber threats are rapidly changing and developing, phishing emails are becoming more sophisticated and training that is several years old might not be sufficient. Training should also be expanded to include education on the signs of an attack.

The impact of threats caused by human mistakes can vary in complexity and consequence. A survey of UK and U.S. employees undertaken by Tessian found that:

- 43% have made digital mistakes that resulted in company or staff repercussions
- 25% confessed to clicking on phishing emails
- Distraction is a huge contributor:
  - 47% believe they clicked on a phishing email due to distraction
  - 57% say they were more distracted when working from home
- 50% of respondents admitted to permitting other people to use their work device

CASE STUDY — INTERNAL THREATS

Maroochy Shire, Queensland

A Disgruntled Former Employee Causes Damage

In 2000, Maroochy Shire in Queensland, Australia faced a series of SCADA attacks. On at least 46 occasions between February and April 2000, the wireless network for the water/wastewater control system was overridden by an attacker resulting in over a million liters of sewage being spilled into local parks, streets, rivers, and the grounds of a hotel.

Maroochy Shire Council had used a contracting firm, Hunter Watertech, to install a SCADA system to control sewage pumps around the town. The system used two-way radio technology to communicate between the pumps. In late January 2000, the system experienced a number of faults: pumps lost control or were disabled, alarms were set off at random, there were communications failures, and pump software configurations were altered.

Initially, staff blamed installation errors and attempted to remedy the errors by reinstalling the software. Police eventually identified Vitek Boden as the person behind the attacks: a disgruntled former Hunter Watertech employee who had lost out on a Council position. Boden used Hunter Watertech equipment and his understanding of the systems to carry out the attacks.

Maroochy Shire Council reported costs of $176,000 from the attacks, including recovery and cybersecurity upgrades. Additionally, Hunter Watertech lost $500,000. Janelle Bryant from the Queensland Environmental Protection Agency said that "Boden's actions were pre-meditated and systematic, causing significant harm to an area enjoyed by young families and other members of the public, marine life died, the creek water turned black and the stench was unbearable."[6]

The Maroochy Shire Council water plants identified significant gaps in their security management controls after the incident:

- Lack of an emergency response plan to deal with security breaches.
- Lack of any security policy, standards or procedures.
- No cybersecurity specialist on staff.
- The SCADA project did not have a cybersecurity risk management plan.

This incident was one of the first ICS attacks and highlighted the severe consequences of weak security. The chief executive of Hunter Watertech, Paul Chisholm, said "With unlimited command of 300 control nodes for both sewage and drinking water, [Boden's] attacks were actually quite restrained. He could have done anything he liked to the fresh water. He faced virtually no obstacles to breaking in."[7]

Lessons Learned

- Cyberattacks can come from anywhere, but those with relevant technology experience pose a larger threat.
- Cybersecurity should also consider partners, the supply chain, and other third parties with remote access and implement appropriate cybersecurity best practices accordingly.
- Former employees and contracts should go through appropriate off-boarding processes to ensure that their institutional knowledge cannot be used against the facility.

3.2 External Threats

External attack types include phishing, malware, DDoS attacks, and ransomware. These threats come from a range of actors including organized crime groups, terrorists, state actors, or opportunistic hackers. Critical infrastructure has not historically been a major target for profiteering groups due to the complexity operations and purpose-built technology, and the relative difficulty of making money from it. However, with the increasing digitization across IT, OT and IoT networks, attackers are becoming increasingly aware of how valuable and vulnerable critical infrastructure can be.

CASE STUDY — EXTERNAL THREATS

Oldsmar, Florida

Abusing Outdated Access Credentials

In 2021, attackers gained access to the water treatment system in Oldsmar, Florida. The threat actors attempted to increase the level of sodium hydroxide from 100 parts per million to 111,000 parts per million. Although the perpetrator has not been identified, analysts believe the intentions were malicious. There are 15,000 people living in the area serviced by this plant, and the consequences could have been serious.

The attack was first identified by an employee who triggered the alarm after noticed a cursor moving across their screen unusually. However, the initial attack was brief and the team believed it had concluded. It wasn't until several hours later that the employees also noticed the attempt to drastically increase the level of chemicals in the water. The first attack would have been a reconnaissance mission to test the vulnerabilities and see what access the attackers could gain.

The hackers had gained entry through the remote access work system at a dam, using software that allows supervisor entry. The software, called TeamViewer, was not designed for use in critical infrastructure. The employees at Oldsmar were unaware that TeamViewer was still in use at the treatment plant, assuming it had been taken offline as workers returned to the office.

"This could've been so much worse,"[8] said David Kennedy, formerly with the National Security Agency (NSA).

Lessons Learned

- Employees should be aware of how to identify an attack and have plans in place should they notice abnormal activity.
- If remote access is needed, it should be designed to work with the specific security needs of the capability and to critical infrastructure standards.
- Software should be constantly monitored to identify aged and vulnerable systems. Unmonitored applications are particularly vulnerable to attack.

CASE STUDY — EXTERNAL THREATS

Bowman Dam, New York

Hacking Into SCADA Systems

In 2013, an undefended computer controlling sluice gates at the Bowman Dam in New was hacked by Iranian actors.[9] The attack by a malicious external state actor had the capacity to cause widespread harm.

The attackers used "Google Hacking" to find weaknesses in security systems. They had searched the internet seeking information on cyber vulnerabilities and identified an entry point for SCADA systems. As there are few manufacturers of SCADA systems, and they typically share similar characteristics and setups, the attacker was able to apply the uniform knowledge to learn about potential entry points and weaknesses.

The hackers accessed the SCADA via a cellular modem, and gained information about "the status and operation of the dam, including information about the water levels and temperature, and the status of the sluice gate, which is responsible for controlling water levels and flow rates."[10] They were also able to view information within the water facility, including usernames and passwords. The hackers had made repeated incursions into the dam over three weeks before the actual attack. The Department of Homeland Security states that the hackers intruded six times before detection.

The effects could have been serious, but during the actual attack, the dam sluice gates were fortuitously offline for scheduled maintenance. A physical disaster was averted, and the incident only cost $30,000 in recovery efforts.[11]

While there the actual damage was limited due to the system being offline, and any attack was not likely to cause huge damage due to the dam's small size, this incident nevertheless demonstrates how easy it can be for a malicious state actor to infiltrate critical infrastructure.

Lessons Learned

- SCADA is used by a range of water capabilities, and it is important to sufficiently customize each to provide individualized defenses. If state actors could gain access to Bowman Dam, they can likely access others.
- Cybersecurity detection technology must be constantly improved—three weeks is too long to let a hack with such serious consequences go undiscovered.
- Critical infrastructure is facing growing cyber threats and must implement disaster recovery plans to avert more serious damage.

4. What Should Organizations Do?

As in all industries, critical infrastructure can best be protected from cybersecurity attacks by planning for them. While a small utility such as Bowman Dam in New York or a wastewater treatment plant in regional Queensland might not realize it's a target, hackers remain opportunistic. Understanding motives of ransomware groups and affiliates, disgruntled employees, or malicious external actors can help to determine specific countermeasures. Businesses often fail to consider the risks from internal threats, but robust protection is necessary based on analysis of both internal and external risk awareness, analysis, and mitigation.

All of the cyberattacks discussed could have been prevented or limited by stronger cybersecurity frameworks. Company executives need to be aware of challenges they may face and proactively champion cybersecurity solutions.

4.1 Identifying an Attack

To plan an attack, threat actors rely on social engineering campaigns to identify patterns and daily routines, as well as review evidence of how a utility has responded to previous attacks. With initial access, threat actors can hunt for credentials to gain privileged access to more systems, and work to identify vulnerable systems to manipulate and either maintain undetected access or masquerade malicious activity as seemingly legitimate.

They also seek to understand how employees communicate with each other to spot weaknesses in the system. Maintaining old practices and failing to update cybersecurity defenses regularly can leave companies vulnerable to attack.

Employees should be educated on what signs to look out for. In the case of Oldsmar, a cursor moving across the screen was the first physical sign of an intrusion.

Employees should be educated on what signs to look out for, in case security mechanisms fail:

- Physical signs:
  - Unactioned security alarms from site access systems and/or cabinet alarms
  - Unauthorized movement detected on a CCTV system
  - Locks that have been re-keyed
  - Damage to or tampering of locks or fencing
  - Computers behaving strangely
- Information, network, and data communications signs:
  - Communications links:
    - Unexplained loss of communications links or strange behavior, for example increased bandwidth usage/telco bills
    - Successful connections to the public internet
  - Field devices: Unusual or unexpected connections to and from
  - Control system: Unusual behavior of devices (input/output commands)
  - Physical assets: Appearing or disappearing in the network, unexplained data

Real-time analysis of operational data is critical to detecting malicious intrusions. Monitoring flow readings, chemical balances in the water supply, and data traffic could provide rapid alerts of a cyberattack. At Maroochy Shire it took months to identify that an attack had even occurred, which led to massive levels of damage and huge costs for the Council.

4.2 Industry Solutions

OT and IoT environment cyber protection in critical infrastructure requires proactive and reactive responses. There is not a 'one-size-fits-all' approach for water utilities as these capabilities range in size and complexity and face different threats. It is essential to review risk mitigation strategies, risk tolerance, and security policy frequently to keep pace with the cybersecurity trends of today. This shouldn't be limited to an understanding of the devices employed; it should include knowledge of the processes underpinning the technology. This will give security teams access to highly accurate detection capabilities and will allow them to provide actionable intelligence when it comes to the most impactful vulnerabilities.

Having a complete understanding of how your system works is critical to identifying weaknesses. A simple mistake such as still having outdated software installed can be costly. Human error contributes to the majority of cyberattacks, so it's important that security hygiene is up to date to best protect staff members. Passwords, a valuable commodity in the cyberspace, need to be strong, and staff need to be educated on the risks of sharing access, with two-factor authentication (2FA) a recommended safeguard. Even well-protected systems can be taken down by clicking on the wrong link, or an opportunistic hacker guessing a simple password.

Flat networks with minimal segmentation can be easily infiltrated. Having critical systems that are not isolated from other applications leaves them vulnerable. By segmenting the network and using technology such as virtual LANs (VLAN) and firewalls, important capabilities can be defended without risk of a weaker segment being infiltrated.

As in the Bowman Dam and Oldsmar cases, once attackers gain an initial foothold in the network, they often perform reconnaissance before undertaking an attack, while avoiding any activity that could trigger anomalies or alarms. This could involve weeks of small intrusions before a cybersecurity system notices. A system which has a built-in anomaly detection, in conjunction with knowledge of the industrial process and normal baseline activity, can identify threats early and identify the malware before it strikes.

Here's What Organizations Can Do To Increase Cybersecurity:

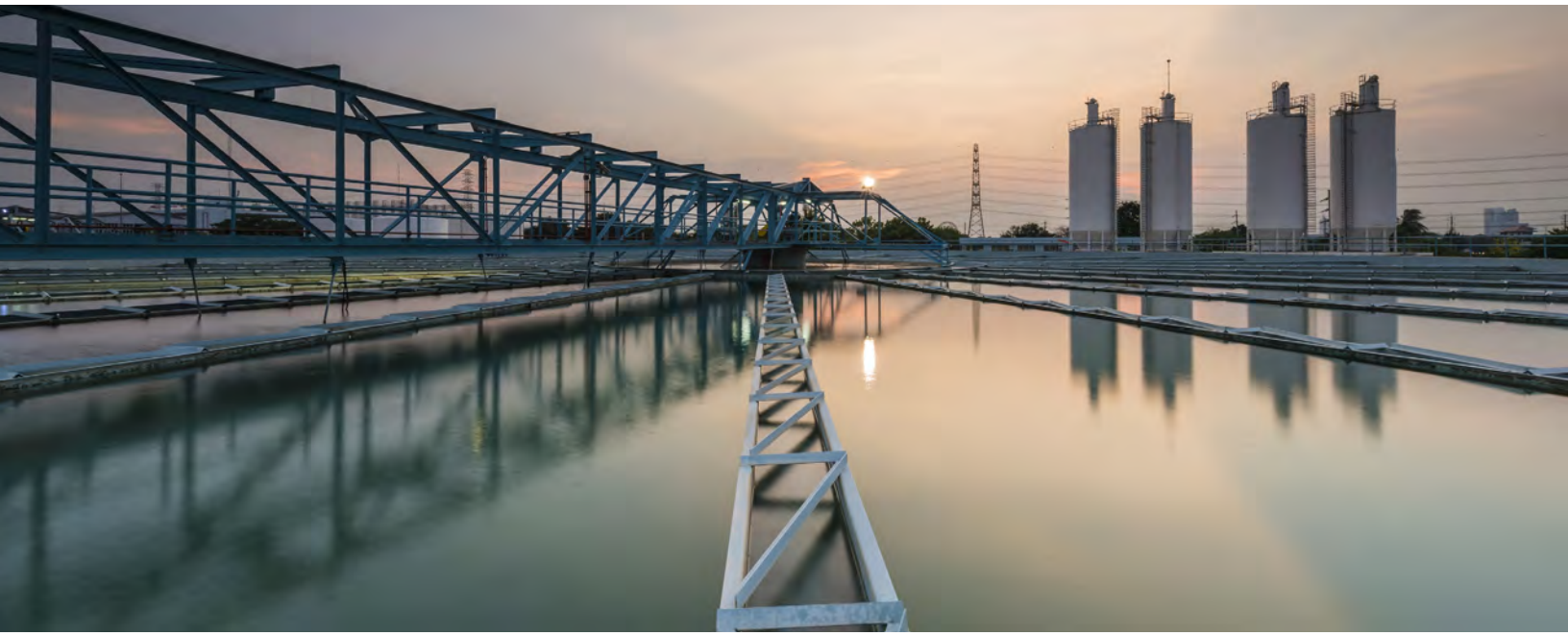
1. Clearly define roles and responsibilities for all stakeholders, including any external providers who may have access to systems.
2. Maintain transparency over all assets and their risk exposure.
3. Implement risk mitigation plans for each asset based on these risk assessments.
4. Maintain a proactive understanding of threat actors and operational risks, and best practices to counter these developing threats.
5. Establish incident response and disaster recovery plans for attack scenarios. Update and test these scenarios regularly.
6. Train all staff on how to identify an attack and what responses to take in the event of an intrusion.
7. Ensure all staff are aware of their own security obligations.

4.3 Implementing Cybersecurity in the Water Sector

Threats are becoming a standard part of the security environment and are a real risk to the physical and economic operation of water utilities. The increasingly complex future environment that the water sector will face places greater demands for effective and capable cybersecurity defenses. The sector needs to be adaptive to change, to deliver a more responsive and efficient cybersecurity defenses.

As interconnectivity and digital dependence increase, and workforces continue the move to remote work, it's crucial that the water industry maintains visibility over the entirety of its operations. Misconfigured firewalls, unpatched systems, out-of-date apps, industrial control systems which aren't suitably adapted to the environment, and simple human error could create flaws and weaknesses in an organization's cybersecurity defense.

The COVID-19 pandemic and global tensions have only exacerbated this trend due to enhanced remote operations and access, and it is critical now more than ever to remain proactive in defending water against cyber threats.



5. References

1. American Water Works Association. 2019. **"Water Sector Cybersecurity Risk Management Guidance."** American Water Works Association. Available at: *https://www.awwa.org/Portals/0/AWWA/ETS/Resources/AWWACybersecurityGuidance2019.pdf*
2. Lin, R. and Fried, R., 2021. **"State of the Water Industry 2021."** Nasdaq. Available at *https://www.nasdaq.com/articles/state-of-the-water-industry-2021-2021-10-04*
3. Deloitte, **"Water Tight 3.0: The top issues in the global water sector."** 2021. Deloitte, *Online version available at https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-water-tight-3-point-0.pdf*
4. Water Sector Coordinating Council. 2021. **"Water and Wastewater Systems: Cybersecurity: State of the Sector."** Water Sector Coordinating Council. Available at *https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf*.
5. Evans, M., Maglaras, L., He, Y. and Janicke, H., 2016. Human behaviour as an aspect of cybersecurity assurance. Security and Communication Networks, 9(17), pp.4667-4679.
6. Theage.com.au. 2002. **"Cyber terrorism a mouse-click away."** The Age. Available at *https://www.theage.com.au/national/cyber-terrorism-a-mouse-click-away-20020708-gdudes.html*.
7. Gellman, B., 2002. **"Cyber-Attacks by Al Qaeda Feared."** The Washington Post. Available at *https://www.tampabay.com/news/pinellas/2021/02/10/oldsmars-water-supply-attack-is-a-warning-experts-say-it-couldve-been-worse/*.
8. Carollo, M. and Evans, J., 2021. **"Oldsmar's water supply attack is a warning, experts say. It could've been worse."** Tampa Bay Times. Available at *https://www.tampabay.com/news/pinellas/2021/02/10/oldsmars-water-supply-attack-is-a-warning-experts-say-it-couldve-been-worse*.
9. Lach, E. 2016. **"Cyber War Comes to the Suburbs."** [online] The New Yorker. Available at *https://www.newyorker.com/tech/annals-of-technology/cyber-war-comes-to-the-suburbs*.
10. Department of Justice. 2016. **"Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector."** Department of Justice. Available at *https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged*
11. Ibid.

NOZOMI NETWORKS

Cybersecurity and Analytics for All Your OT & IoT Connected Devices

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NN-WATER-UTILITIES-IB-8.5x11-001

nozominetworks.com